การไฟฟ้าส่วนภูมิภาค

PROVINCIAL ELECTRICITY AUTHORITY

ประกวดราคาเลขที่ PEA-DDIP-DDC-1/2018
จ้างจัดหาพร้อมติดตั้ง Hardware และ Software ระบบศูนย์สั่งการจ่ายไฟ (SCADA/TDMS)
ด้วยวิธีการทางอิเล็กทรอนิกส์

โครงการเพิ่มประสิทธิภาพระบบศูนย์สั่งการจ่ายไฟ (ด้านระบบศูนย์สั่งการจ่ายไฟ)

DISTRIBUTION SYSTEM DISPATCHING CENTER IMPROVEMENT PROJECT (DISTRIBUTION DISPATCHING CENTER)

เล่มที่ 4

บทที่ 10 : Technical Specifications

Part B : SCADA/TDMS

สำนักงานโครงการ คปศ – ด้านระบบศูนย์สั่งการจ่ายไฟ
200 ถนนงามวงศ์วาน จตุจักร กรุงเทพมหานคร 10900
DDIP/DDC PROJECT OFFICE
200 NGAM WONG WAN ROAD, CHATUCHAK,
BANGKOK 10900, THAILAND
www.pea.co.th
TEL: 0-2590-5807, 0-2590-9501 FAX: 0-2590-9174

รายการเอกสารประกวดราคา

เล่มที่ 1 เงื่อนไขประกวดราคา

เล่มที่ 2 PRICE SCHEDULES

เล่มที่ 3 TECHNICAL SPECIFICATIONS

เล่มที่ 4 TECHNICAL SPECIFICATIONS

บทที่ 10: Technical Specifications
Part B: SCADA/TDMS

Table of Contents

List of Exhibits:

1. Introduction

This Part B of the Technical Specifications concerns the Transmission and Distribution Management System (TDMS). As part of the Distribution Dispatching Center Improvement Project (DDIP), the TDMS will replace the SCADA/EMS/DMS system in the System Management Center (SMC) at Authority headquarters in Bangkok, the SCADA/DMS systems in twelve (12) Area Distribution Dispatching Centers (ADDCs) located throughout Thailand, and the SCADA/DMS system in the Phuket Distribution Dispatching Center (PDDC), which falls within the responsibilities of ADDC-S2, i.e., the ADDC in the Authority's Southern Region Area 2. For additional DDIP information, refer to Part A of the Technical Specifications, Project Overview.

The TDMS shall allow the Authority to consolidate its power system operations in such a way that all fourteen (14) control centers will be served by fully-integrated SCADA/EMS/DMS server platforms located at two (2) new Authority data centers[1]. On this basis, the dispatchers at each control center will utilize the SCADA, EMS, and DMS applications hosted on these platforms from new remote client workstations. On cutover to the TDMS, the existing control center systems will be dismantled.

2. TDMS Backup Concept

The TDMS hardware and software at each new data center shall be a replica (mirror image) of the hardware and software at the other data center. To support critical TDMS functionality, application servers at each data center shall be redundant. Moreover, dispatchers at the control centers shall be provided with bump-less access to critical SCADA, EMS, or DMS applications in the event any of these applications can no longer execute on any of the redundant servers in which they are installed at one data center and must therefore execute on one of the corresponding redundant servers at the other data center. This backup/failover feature shall also apply to other critical functions and processes requiring unlimited access to system resources. The way in which the Contractor's solution meets the backup/failover feature shall have been clearly described in the Contractor's proposal and shall be demonstrated during system implementation. Demonstration shall include the worst-case disaster recovery scenario in which all facilities at one of the data centers become unavailable.

3. Data Center Configuration

This clause presents a conceptual high-level overview of each TDMS data center from a server configuration perspective.

3.1 General Concept

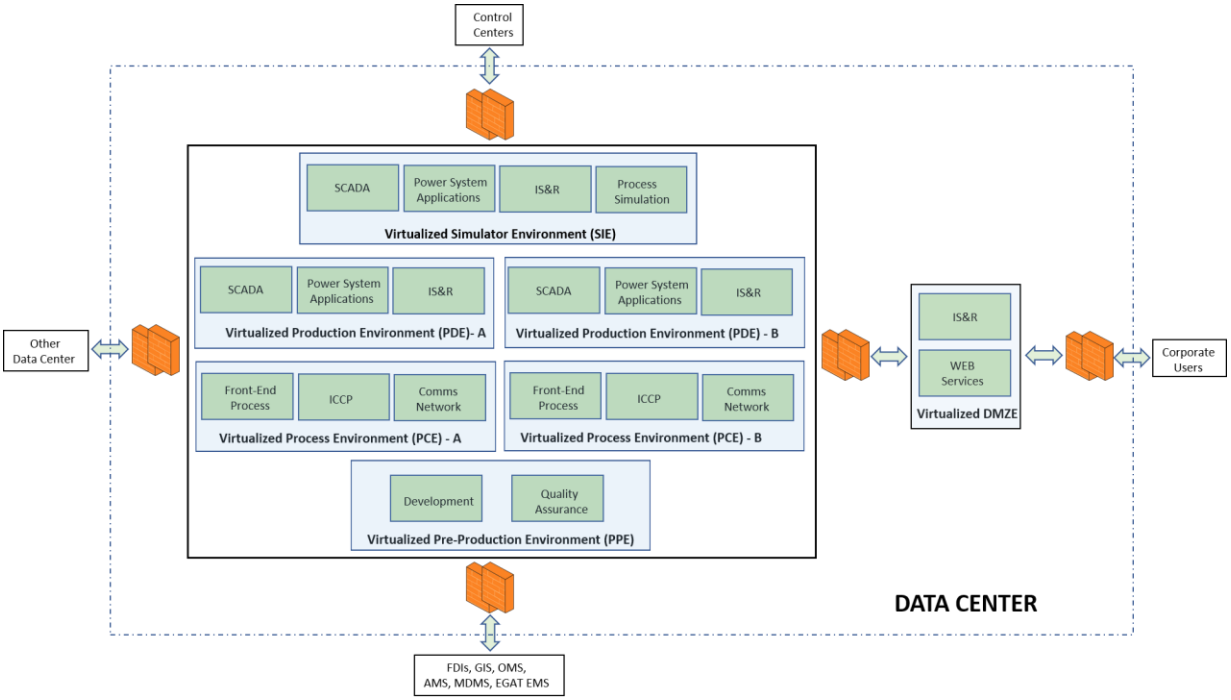
In general, the TDMS platform at each data center shall consist of virtual machines configured on several physical servers and interconnected via redundant Virtual Local Area Networks (VLANs) suitably segregated and secure to meet the System's functional requirements.

[1] *The building of one data center is on-going and is expected to be completed well in time to accommodate installation of its DDIP hardware and software. If the other data center is not available in time, the Authority will provide a suitable temporary locatio*n.

A conceptual configuration based on server virtualization is illustrated in Exhibit 3-1, noting that the exhibit does not identify servers such as those as may be required to support the User Interface facilities located remotely at the SMC and ADDCs.

Thus, the following virtual environments are identified noting, however, that these are provisional, i.e., the physical and virtual environments ultimately implemented shall be based on the Contractor's optimized configuration as proposed and possibly modified, with Authority approval, during the project's design phase. For example, it would be acceptable if all instances of the IS&R function were to be hosted entirely on a physical server provided that the Contractor's proposed configuration supports the Authority's specified TDMS security, capacity, performance, and availability requirements.

Exhibit 3-1: Data Center Virtual Environment Concept



3.1.1 Production Environment (PDE)

This virtualized, redundant environment shall host the SCADA, EMS/HV, and DMS/MV functions that dispatchers and others shall access remotely and securely from any of the Authority's 14 control centers. It shall also host the database that the PDE functions depend upon, a database that contains, for example, real-time telemetered and power system network modeling data.

Independently of the PPE (refer to Clause 3.1.3.1), the PDE shall include a TDMS Editor tool capable of updating or changing the structure and content of the database. This capability shall support permanent database updates or changes to reflect existing, i.e., actual, operational conditions such as those that relate to newly installed or removed power system equipment. In addition, for study purposes, it shall support installation and removal of non-existing power system equipment, such equipment being distinguished by a readily recognized identification feature.

As a virtualized PDE component, the SCADA server shall receive power system data, send power system control commands, and exchange data with other systems via the TDMS platform's Process Environment (PCE). This shall include support for PDE's interoperation with power system devices and the Authority's Advanced Metering Infrastucture (AMI) facilities such as the Meter Data Management System (MDMS) or its associated Head-End Systems. It shall also include the capability to exchange data with the SCADA/EMS at the control center belonging to the Electricity Generation Authority of Thailand (EGAT) as well as the Authority's Outage Management System (OMS) and Asset Management System (AMS).

Other virtualized servers shall be used to execute the HV/MV Applications and the Information Storage and Retrieval (IS&R) function. This shall include application/function execution in required real-time and study modes. As described elsewhere in these Technical Specifications, the virtualized server for the IS&R function shall take the form of a high-speed, high-capacity, Data Historian.

In addition to the above, the PDE shall be the source of power system operations data to be accessed securely via each TDMS platform's Demilitarized Zone Environment (DMZE), i.e., by properly authorized Authority personnel on the Corporate Wide-Area Network (WAN).

3.1.2 Process Environment (PCE)

This virtualized, redundant environment shall host functions used for real-time and near real-time data communications.

Real-time data communications shall support TDMS interoperation with the following types of Field Device Interfaces (FDIs):

1) Computer-Based Substation Control Systems (CSCSs) at Authority HV and HV/MV substations.

2) Substation Remote Terminal Units (SRTUs) at Authority HV and HV/MV substations.

3) Feeder RTUs (FRTUs) or Feeder Device Control Units (FDCUs) at sites where Line Reclosers (LRCs), Remote Controlled Switches (RCSs), Line Recloser/Regulators (LRRs), and Switched Capacitor Banks (SCBs) are deployed along Authority MV feeders, where RCS is a term used by the Authority to denote a Load Break Switch (LBS).

4) FRTUs or FDCUs at Distributed Energy Resource (DER) points of connection with the Authority's HV and MV power system circuits. As also referred to as Distributed Generators (DGs), DERs of capacity greater than 10 MW are owned and operated by Small Power Producers (SPPs). DERs of capacity less than 10 MW are owned and operated by Very Small Power Producers (VSPPs). DERs include diesel generator, Solar-PV, and Wind-Turbine units. In addition to supporting DER monitoring and on/off control, such FDIs in the future may support more complex Distributed Energy Resource Management System (DERMS) functionality, integrated as part of the TDMS to optimize utilization of DERs. In this respect, DERMs may also accommodate future Demand Response (DR) programs.

5) FRTUs or FDCUs at microgrid points of connection with the Authority's HV power system circuits.

6) FRTUs or FDCUs that will allow the TDMS to interoperate with autonomous decentralized feeder self-healing functions that the Authority may implement in the future.

With reference to Exhibit 3-1, the virtualized Communication Network Processors (CNPs) of PCE shall be used to communicate with the SCB FDIs whereas, for all other FDIs above, the virtualized Front-End Processors (FEPs) shall be used.

To support communications between the CNPs and SCB FDIs, the Authority shall arrange for the cellular networks of local service providers to be available. Otherwise, communications between the FEPs and the other FDIs shall use the Authority's high-speed Optical Fiber (OFB) backbone communications network augmented, where necessary, by the Wireless (WRL) communication cells to be provided by others as part of DDIP (refer to Part A of the Technical Specifications). As all communication circuits terminating at a Front-End Processor (FEP) will be IP-based, the communications protocol shall be the latest secure authentication version of DNP 3.0 over IP.

The CNPs shall also be used for data communications between the TDMS and the Authority's AMI facilities. In addition, the CNP is assumed to be used for data exchange between the two data centers, this data supporting center-to-center synchronization and the required center-to-center failover capabilities.

The PCE shall include the virtualized ICCP server for data exchange with the Authority's OMS and EGAT's SCADA/EMS. For this purpose, the secure Inter-Control Center Communications Protocol (ICCP) shall be used.

Note that all PCE external data sources will have the capability to feed both data centers. Apart from the data sources on MV feeders, which will communicate in part over the Authority's WRL network, or entirely over the cellular networks of service providers, all other data sources will communicate over the Corporate WAN consisting of high-speed OFB backbone communication circuits. Data rates for the WRL network will not be more than 38.4 kbps.

3.1.3 Pre-Production Environment (PPE)

As a minimum, this virtualized but non-redundant environment shall consist of one or more virtualized servers supporting Development System (DVS) and Quality Assurance System (QAS) functions.

3.1.3.1 DVS Functions

The DVS, as a minimum, shall include a virtualized server hosting the data engineering functions and tools supporting off-line development of the databases and displays (both geographical and schematic) that are required by the SCADA, EMS, and DMS applications used by the QAS, PDE, and SIE. The databases shall include, for example, all necessary power system network and device modelling data along with the associated I/O points provided by the Authority's FDIs.

Development shall include initial database and display creation using static power system network data imported from the Authority's GIS followed by validation and any necessary correction or augmentation procedures. In addition, it shall include the capability to update the databases and displays based on incremental data imports from the GIS. For Corporate users of the TDMS, web-based displays shall also be developed, including those in the form of customized dashboards.

On completion, databases and displays shall be exported for utilization in the QAS and ultimately in the PDE and SIE. They shall also be used for factory development and testing of the PDE and SIE.

Development shall include the capability to create and update databases and displays independently of the GIS. For example, the DVS shall host a TDMS Editor tool that shall enable display and database details corresponding to the power system's network model and its associated field devices and I/O points to be prepared off-line, validated via the QAS, and then loaded to create, update, or replace the on-line displays and databases in the PDE and SIE.

3.1.3.2 QAS Functions

The QAS shall include virtualized servers hosting functions that replicate the PDE such that these functions can be used to test SCADA, EMS, and/or DMS functionality, including any software, database, and display updates, prior to installation and execution in the PDE and SIE. For example, it shall be used to conduct initial point-to-point testing of new or modified RTUs or to test software patches, including those for fixing TDMS vulnerability to a security threat, before these RTUs or software patches are deployed for the PDE and SIE. The QAS shall also support the creation and testing of reports to be generated by the PDE and SIE and, to the extent possible, TDMS interfaces with the Authority MDMS and OMS systems and the EGAT SCADA/EMS.

Following any new RTU, software, database, or display deployment for the PDE, an important feature of the PDE and PPE, in case such deployment proves problematic, shall be the capability to roll back the deployment so that the PDE returns seamlessly to its former on-line state.

3.1.4 DMZ Environment (DMZE)

This virtualized, non-redundant environment shall host a virtualized Web Server and a high-speed, high capacity Data Historian used to execute a replicated instance of PDE's IS&R function. These servers shall meet the needs of users on the Corporate WAN who are authorized to access near real-time, calculated, and historical data provided securely from the TDMS, i.e., on a read-only basis. Such users shall in no way be able to access any other servers comprising the TDMS, i.e., those within the power system Electronic Security Perimeter (ESP).

3.1.5 System Management Environment (SME)

This virtualized, non-redundant environment shall include centralized Network Management System (NMS) functions for the configuration, control, and performance monitoring of TDMS resources including servers, processors, peripheral devices such as firewalls, network devices such as routers and switches, applications, and databases. These functions shall be accessible by authorized users from any TDMS workstation and shall be used to manage resources anywhere in the network subject to access security constraints.

The SME shall also include a unified Cyber Security Management System (CSMS) that shall alert administrators and dispatchers in the event a security threat is detected. Conceptually, as in Exhibit 3-1, it shall include a virtualized Authentication Server as well as a virtualized CSMS server. These servers shall be used to support the security requirements as specified elsewhere in these Technical Specifications (refer to Clause 7 and Clause 11).

The SME functions shall have the capability to control any number of resident application systems by the installation of different driving tables that define the makeup of an application system, the assignment of processes to servers, and the requirements for network resources. This shall be achieved without requiring source code changes. The functions shall facilitate the orderly start-up, shutdown, and tuning of any TDMS resource without affecting the availability of other elements of the TDMS.

Commercially available, standards-based network management products are preferred, particularly products employing the SNMP version 3 (SNMPv3) standard. All TDMS resources shall include SNMP agents for use by the SME functions and by the associated Contractor-supplied management tools. In this respect, a graphics-based user interface for TDMS management shall be provided instead of a command line interface.

The SME shall “discover” TDMS resources automatically and shall have the capability to automatically configure these resources. It shall also be possible to add resources outside the TDMS to the SME scheme. This may require modifications to the outside applications, databases, processors, or devices, such as the addition of agents or other software plug-ins, and all necessary cyber security measures shall be provided.

Within this context, the Contractor’s proposal shall have described all functional capabilities as offered to satisfy the SME requirements. This shall include its security related features as applicable to SME interfaces with both TDMS and non-TDMS resources.

All errors and other events detected by the SME functions shall be recorded and reported to the user. Fatal errors shall be reported as alarms. Where an error causes the functions to reconfigure the TDMS (such as bringing a backup resource to the primary state), the reconfiguring action shall be reported as an alarm along with an error report. Such error reports and other log messages shall be able to be recorded by the IS&R function for audit and troubleshooting purposes.

3.1.6 Simulator Environment (SIE)

This virtualized, non-redundant environment shall provide Operations Training Simulator (OTS) functionality allowing transmission and distribution personnel and other users to run the SCADA, EMS, and DMS real-time, study, and IS&R functions against a power system network model that simulates the dynamic behavior of the network in response to various user-defined operating conditions. In this respect, it shall include a virtualized Process Simulation Server (PSS) to feed SCADA with postulated input values and events, such as time-dependent load profiles and breaker trips, in the form of a pre-defined simulation scenario. The capability shall be provided to introduce such input during an on-going simulation session as well. A simulation session may start, for example, from a saved base case or snapshot taken from the on-line TDMS or from a previous simulation session.

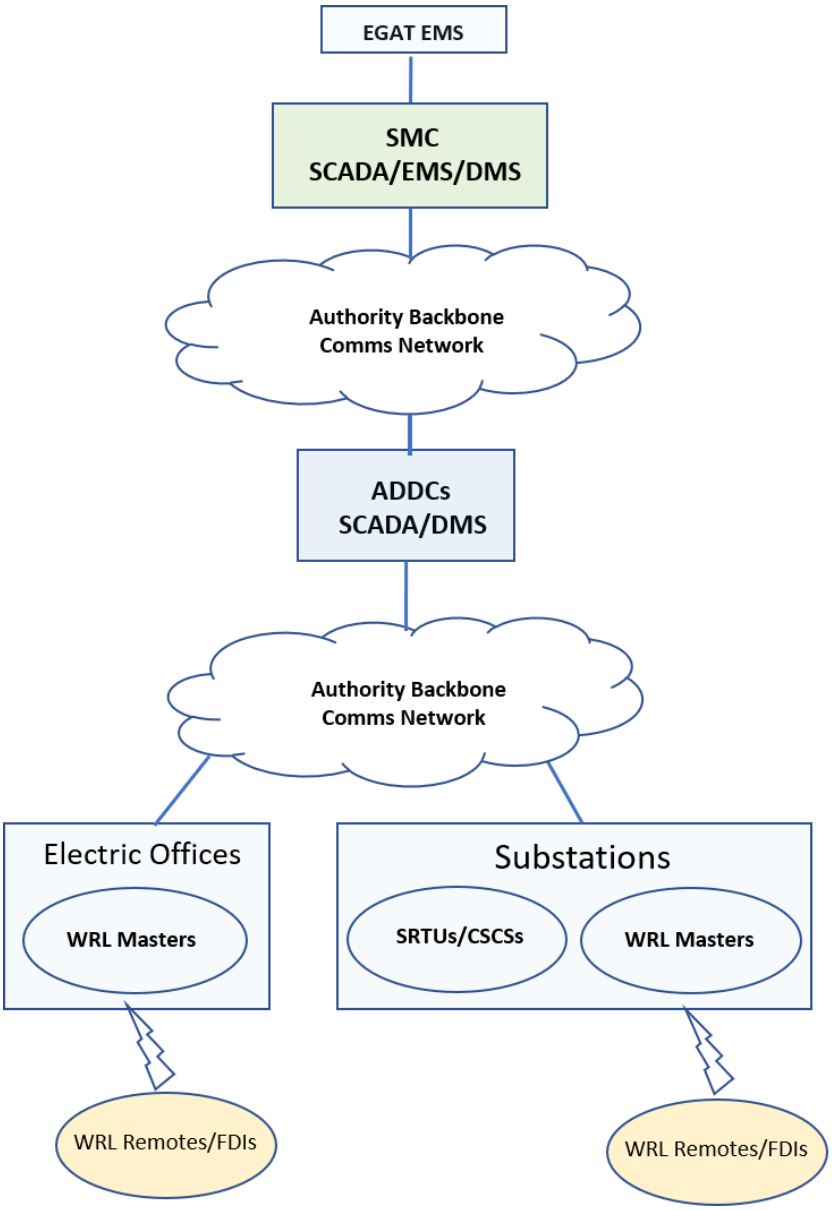
Typically, simulation sessions shall be run to train dispatchers in the presence of a trainer, who will be responsible for creating the simulation scenarios as well as interacting with the trainees. In addition, a dispatcher or any other authorized user shall be able set up and run a simulation session independently, i.e., for self-training or self-study purposes (refer to Clause 20.23).

4. System-Wide Architecture

The TDMS shall realize a completely different system-wide architecture compared to the existing architectures resulting from the Authority's 1st and 2nd Stage Distribution Dispatching Center (DDC) projects, referred to herein as DDC1 and DDC2.

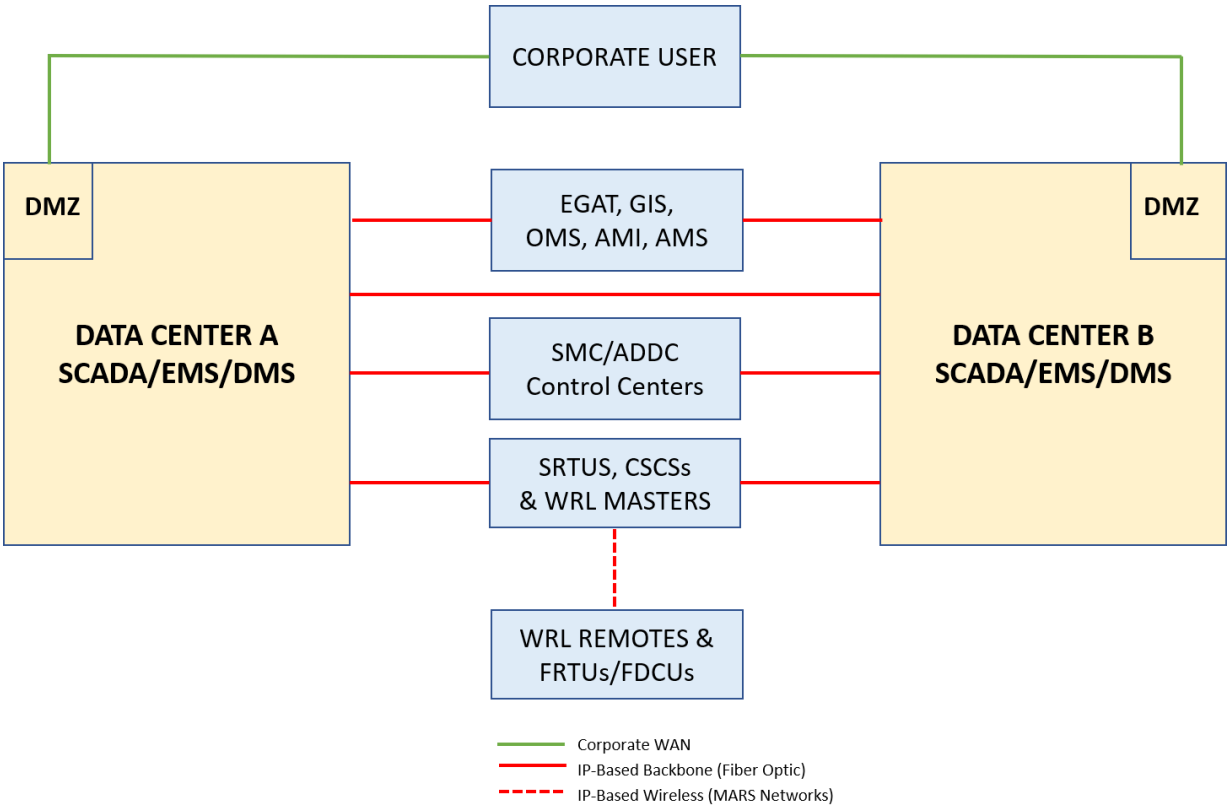
The DDC1 and DDC2 architectures are based on SCADA/DMS/EMS or SCADA/DMS servers located at each control center. Thus, as shown in Exhibit 4-1, these servers receive, process, store, and display data for use by their own dispatcher and data engineering personnel based on interoperations with their own set of FDIs, such as SRTUs, CSCSs, FDCUs, and FRTUs. SCADA/EMS/DMS interconnections with EGAT's SCADA/EMS as well as the SCADA/DMS systems are supported. Interconnections between the DDC1 and DDC2 systems and the Authority's existing GIS and OMS systems are also supported but, for simplicity, are not included in Exhibit 4-1.

Exhibit 4-1: DDC1/DDC2 Existing Architecture (Conceptual)



In contrast, as shown in Exhibit 4-2, the architecture resulting from DDIP shall lead to a situation in which only the TDMS servers at the two data centers shall interoperate with the substation and feeder located FDIs, the EGAT SCADA/EMS, and the Authority's GIS and OMS. In this respect, the FDIs represent not only SRTU, CSCS, FDCU, and FRTU devices, but also any new type of device as may be used for TDMS interoperation with microgrid, Distributed Energy Resource (DER), and Demand Response controllers. As in Exhibit 4-2, DDIP shall also provide the new capability that is required to support TDMS interoperation with Authority AMI and AMS facilities.

Exhibit 4-2: TDMS System-Wide Architecture (Conceptual)



Given the DDIP architecture, users of the new dispatcher and data engineering remote workstations at each DDC1 and DDC2 control center shall be supported by the same common set of TDMS data center servers rather than by separate SCADA/EMS/DMS or SCADA/DMS servers as currently exist at these control centers.

The TDMS architecture in comparison to the existing DDC1 and DDC2 architectures shall provide system backup capabilities from a control center perspective as well as data center perspective. Thus, as the remote workstations to be installed at control centers shall be supported by common SCADA/DMS/EMS applications, displays, and databases (including power system network models and I/O points), the TDMS shall allow dispatchers at one or more of the control centers (provided they are properly authorized) to take over the role of dispatchers at any control center that becomes non-operational.

The TDMS architecture shall also support more manageable system maintenance activities in that TDMS application software, displays, and databases need only be maintained at the two data centers, whereas in the existing DDC1/DDC2 architecture such maintenance is performed and coordinated at fourteen (14) individual control centers. The new maintenance activities, utilizing a TDMS Editor provided by the Contractor on data center PPE servers, for example, shall be possible from any control center data engineering workstation.

In addition to the capabilities and features described above, the TDMS architecture shall help simplify implementation of the Authority's Enterprise Application Integration (EAI) objectives. Relevant DDIP interoperability (system integration) requirements are specified in Clause 12.

Another important feature associated with the new architecture is that all data communications between the TDMS and its associated Substations and Electric Offices, i.e., over the Authority's Optical Fiber Backbone (OFB) communications system, will be IP-based. The new UHF wireless communications system, provided by other DDIP contractors to allow the TDMS to reach feeder located FDIs, will be IP-based as well. Thus, the TDMS need only support IP-based communications.

To support the TDMS architecture, the intent of the Authority is to also ensure that the communication systems and field device interfaces can support interoperation with both data centers, e.g., all data from field device interfaces at substations and feeder locations will be made available to both data centers. In this respect, the TDMS servers at each data center shall be able to collect the same real-time data and, with appropriate interlocking, send commands to operate any of the project's substation and feeder located devices.

5. Server Requirements

This clause provides a high-level description of the requirements that apply to the TDMS servers to be supplied and installed by the Contractor at the project's two data centers.

These requirements are based on the Authority's strong preference for a server infrastructure that is virtualized. As already indicated in Clause 3.1, this infrastructure consists of physical servers hosting multiple Virtual Machines (VMs) in the form of guest software dedicated to specific TDMS functions and tasks. Alternatively, the Contractor's proposed solution may be in the form of a traditional non-virtualized infrastructure in which physical servers distributed on redundant LANs are dedicated to specific TDMS functions and tasks. A mix of virtualized and non-virtualized infrastructures may also apply. For example, a physical (non-virtualized) high-speed, high-capacity Data Historian and Web Server in each TDMS Demilitarized Zone (DMZ) are acceptable.

Whether virtualized or physical, the server infrastructure including its detailed configuration design shall have been proposed by the Contractor for the express purpose of satisfying in the best possible way the Authority's TDMS capacity, performance, availability, and security requirements.

5.1 Host Servers

As a minimum, the physical or host servers comprising the virtualized environments of the two TDMS data centers shall exhibit the following capabilities and features:

1) Recovery of a failed host shall include start-up and re-synchronization without interruption to existing online or offline operations.

2) Each host server shall include Operating System, RAM, Solid State Drives (SSDs), VMs, Network Interface Cards (NICs), and Virtual Machine Manager (VMM) software. The Authority's SSD auxiliary memory preference is that which utilizes Non-Volatile Memory Express (NVme) technology.

3) The Operating System for all hosts shall be the same revision of a widely accepted and latest version of the Linux operating system, with long term support from a Recognized Distribution such as Red Hat Enterprise Linux or SUSE Linux Enterprise Server. Alternatively, the same

revision of the latest Windows Server operating system, with long term support from Microsoft, shall be used. The Operating System shall be a standard product and shall not be modified by the Contractor.

4) The same revision of a widely accepted Virtual Machine Manager (VMM) platform shall be utilized in each host server. For VMM details refer to Clause 5.3.

5.2 Virtual Machines

The number of Virtual Machines (VMs) performing various TDMS functional tasks on each host server shall be based on the Contractor's proposed design. In this respect, as in determining the number of hosts, due consideration shall have been given to the TDMS capacity, performance, availability, and security requirements. The Contractor's proposal shall have clearly justified the design from the perspective of how the virtualized infrastructure supports:

1) Balanced functional task sharing.

2) Comprehensive backup and disaster recovery capabilities.

3) Convenient system administration and maintenance procedures.

As a provisional design, the Contractor's virtualized infrastructure at both data centers shall be based on the following principles (also refer to Clause 5.3):

1) Each host server shall host one or more Virtual Machines such that each VM shall perform a specific functional task or group of tasks.

2) Redundant host servers shall be configured with corresponding VMs that are replicated in precisely the same way.

3) Each VM shall support virtualized Operating System, RAM, Solid State Drive (NVMe preferred), and NIC functionality.

4) The Operating System functionality for all VMs shall correspond to the same revision of a standard (unmodified) Linux or Windows operating system that is both current and known to have long-term support.

5) Support for OS-level virtualization such that an OS cannot read a memory area of another OS running another application.

6) SNMP and API support for integration into a Network Operations Center (NOC) environment.

5.3 Virtual Machine Manager

The Virtual Machine Manager (VMM) shall provide server virtualization and hypervisor management facilities based on the latest version of a suitable third-party product. The VMM shall be able to operate on hardware products from at least 3 different OEMs, i.e., a VVM that can only be used on one specific hardware product is not acceptable.

Augmented by Contractor proprietary software where necessary, e.g., to support backup and failover, the VMM shall support as a minimum:

1) Installation of operating systems as hosted VMs.

2) Configuration of multiple individual guest VMs on each host server, i.e., configuration of their separate virtualized CPU, RAM, Solid State Drive, and NIC parameters.

3) Configuration of each guest VM using multiple virtualized CPUs (vCPUs) depending on the workload.

4) Optimization of VM memory usage such as dynamic memory control within minimum and maximum limits.

5) Management of pooled host server resources. This shall include management of:

    a) VM cloning.

    b) VM migration from one host to another.

    c) VM export/import facilities.

    d) Physical network connections.

    e) Network configuration and storage sharing.

    f) Computational load sharing among VMs and VM hosts.

    g) TDMS backup and disaster recovery facilities including, for example, host monitoring, host automatic shutdown if impaired, and VM restarting on an alternative healthy host if necessary.

    h) Start up and re-synchronization of failed resources without disruption to on-going operations.

    i) Local access to the TDMS data center servers by system administration and maintenance personnel.

    j) Secure remote user access to TDMS functionality from control room dispatcher and data engineering workstations based on areas of responsibility (also referred to as areas of jurisdiction) as well as individual roles and permissions.

    k) Security features such as encryption, Lightweight Directory Access Protocol (LDAP) authentication of users, role based VM access, HTPS using CA (SSL), 802.1q VLAN segmentation, and Syslog.

6. Remote Workstation Requirements

6.1 Control Center Workstations

The TDMS shall include the capability of users located in the SMC and ADDC control centers to access the functional capabilities and features of the data center servers remotely as required to monitor and control power system operations and conduct system administration, maintenance, and troubleshooting activities. In this respect:

1) Remote access to the TDMS servers shall be supported from dispatcher and data engineering workstations provided by the Contractor.

2) Each workstation shall interoperate with the data center servers as a remote client.

3) Each workstation shall include a floor-standing desktop (tower) PC with monitors, keyboard, and mouse. The dispatcher workstations shall include 3 monitors. The data engineering workstations shall include 2 monitors.

4) The new dispatcher workstations shall be used in place of the existing dispatcher workstations in every control room and shall be installed together with new console furniture providing, as a minimum, necessary desk-top space, storage facilities, and chair.

5) The new data engineering workstations shall be used in place of the existing data engineering workstations in the DDC1 and DDC2 control centers. In this case, no new furniture is required, i.e., existing desks and chairs will be utilized.

6) Each data engineering workstation shall be supported by an individual Contractor provided UPS.

7) Each workstation Operating System shall be the same as used by the VMs, i.e., a current long-term supported version of Linux or Windows.

8) Workstation connections to the data centers shall be controlled in such a way that they are automatically connected to appropriate data center services depending on specific user roles and permissions. Subject to Authority approval, this shall include a secure Contractor-proposed two-factor authentication procedure. If necessary, VPN connections shall also apply.

9) Remote client access to the TDMS servers may use Contractor proprietary software or third-party Virtual Desktop Infrastructure (VDI) software such as Microsoft Remote Desktop, Citrix Independent Computing Architecture (ICA), Virtual Network Computing (VNC), or similar.

10) Remote workstation software shall be capable of being installed, maintained, and administered from any designated control center such as the SMC or one of the ADDCs.

6.2 Training Center Workstations

The TDMS shall provide users (such as trainers and trainees) in the Authority's training center, which is in close vicinity to the Authority's C3 area control center, with access to the data center servers supporting the capabilities and features of the OTS functionality provided by the SIE. In this respect:

1) Remote access to OTS functionality shall be supported from trainer/trainee workstations provided by the Contractor.

2) Each workstation shall interoperate with the appropriate data center servers as a remote client.

3) Each workstation shall include a floor-standing desktop (tower) PC with three monitors, a keyboard, and mouse.

4) For each workstation, console furniture (including desk-top space, storage facilities, and chair) will be provided by the Authority.

5) Each workstation Operating System shall be the same as used by the VMs, i.e., a current long-term supported version of Linux or Windows.

6) Workstation connections to the data centers shall be controlled in such a way that they are automatically connected to appropriate data center services depending on specific user roles and permissions. Subject to Authority approval, this shall include a secure Contractor-proposed two-factor authentication procedure. If necessary, VPN connections shall also apply.

7) Remote client access to the TDMS servers may use Contractor proprietary software or third-party Virtual Desktop Infrastructure (VDI) software such as Microsoft Remote Desktop, Citrix Independent Computing Architecture (ICA), Virtual Network Computing (VNC), or similar.

8) Remote workstation software shall be capable of being installed, maintained, and administered from a designated control center such as the SMC or one of the ADDCs.

7. Security Architecture

The component systems and equipment comprising the TDMS shall be contained in clearly defined electronic security perimeters. All systems and equipment located within each security perimeter, as well as the equipment that defines the security perimeter, shall be treated and configured as Critical Cyber Assets. In this respect, based on applicable standards and best practices, the Contractor's proposal shall have provided documents and drawings depicting all electronic security perimeters used to protect the TDMS, all interconnected TDMS components within these perimeters (such as the virtualized environments comprising each data center), all interfaces serving as perimeter points of access, and all equipment deployed or configured for controlling and monitoring access to the components within each perimeter.

Interfaces allowing access to the systems and equipment within electronic perimeters shall be protected by next-generation firewalls and associated intrusion prevention, detection, reporting, and mitigation

software. For example, firewalls shall be used to help protect the TDMS from unauthorized access from field device locations.

The Contractor shall assist the Authority in determining the minimum required access permissions for the firewalls to allow functional yet secure operation of the TDMS, including normal, emergency, and required maintenance actions.

Where external access to systems and equipment within an electronic security perimeter can take place, strong technical controls are required to ensure the authenticity of the accessing party. As specified elsewhere in these Technical Specifications, this includes a secure two-factor authentication method that augments static user names and passwords.

Where applicable, the Contractor shall propose additional security measures to provide external user access to data without affecting the performance, reliability, or security of the TDMS. DMZ configurations shall be implemented in such a way as to maximize the security of the TDMS while facilitating external user access to only the data resources located within the DMZ.

All firewalls shall be implemented using a "default deny" philosophy, allowing access for only those users, nodes, ports, and services that are specifically allowed such access. All supplied firewalls and associated routers shall be configured to generate log entries on attempted as well as successful unauthorized access. The Contractor shall provide a list of all necessary and required ports, services, and addresses requiring access through all firewalls supporting normal, emergency, and ongoing maintenance functions. All access implemented during system development, factory test, and site test activities shall be documented and reviewed for removal prior to system commissioning.

The electronic security perimeters shall have the following characteristics as a minimum:

1) No direct connection from the Internet to the TDMS, and vice versa. Where the TDMS requires support from the Internet, access to Google maps for example, such access shall require appropriate security measures to be implemented.

2) Users on the Corporate WAN shall not have direct query or access capability to any data or processes within the TDMS. Corporate users shall only have access to data available from the Historian and/or Web servers in the DMZ.

3) Well-defined rules outlining required and authorized traffic must be implemented at all access points.

4) Management of access control devices must be permitted only from a highly-restricted subset of management devices.

5) Provisions to record all network traffic for detecting unauthorized activity, unusual activity, and attempts to defeat the security capabilities of the TDMS. The Contractor shall propose a mechanism for determining what network traffic patterns constitute "normal" traffic.

8. Software Architecture

A distributed computing environment shall ensure adequate flexibility for TDMS evolution. The distributed computing environment shall allow TDMS resources at both data centers to be used transparently from all remote workstations such that there will be no restrictions on the geographic dispersal of applications and data among the servers of the TDMS.

8.1 Open System Interfaces

The Authority requires documented APIs and a programming environment within the TDMS that includes, for example, standard ODBC, SQL, DDE, and XML interfaces to support the goals of integrating applications and allowing access to the database. In this respect, the distributed computing environment shall allow hardware or application software additions, whether supplied by the Contractor or obtained from third party vendors, both for capacity expansion and functional upgrades with a minimum effect on existing TDMS components or operations.

To meet the Authority's distributed and open-system requirements, the following design concepts shall apply:

1) A TDMS based on Open System Standards or have a clear migration path toward an open architecture in which the software is totally transparent of the hardware, such that any hardware adhering to these standards can be replaced or upgraded with a functionally similar device not necessarily of the same original manufacture.

2) Major subsystems distributed to different sets of networked servers (whether virtualized or physical) such as those that support SCADA, network analysis functions, and user interfaces (e.g., from remote workstations).

3) All software written in standard high-level languages.

4) A design providing the highest possible level of hardware and software independence through use of standard products, standard toolkits, and application modularity.

5) Expansion of power system models in the TDMS accomplished simply and quickly without need for any recompilation or restart.

6) Capability to run TDMS software in test mode without affecting the on-line system.

Programming interfaces for the following functions are also required with respect to each TDMS programming language:

1) *Database access* – Read and write all attributes of database items.

2) *Supervisory controls* – Initiate supervisory control commands and receive reports on supervisory control actions.

3) *Tagging* – Place and remove tags.

4) *Data processing* – Process database items produced by a function as in passing items to data processing routines such as conversion to engineering units, limit checking, and storage in the database.

5) *Alarming* – Initiate and manage alarms.

6) *Application program controls* – Initiate, schedule, and terminate TDMS applications.

7) *User interface* – Manage user interface windows and their contents, and initiate programs associated with displays. Such program control action shall include initiating programs when a display is opened, when a display is closed (or replaced by another display), and when commanded by a user from a display.

8) *Periodic data collection* – Initiate and suspend periodic data collection. In addition, the interface shall facilitate initiation of single (non-periodic or "demand") executions aimed at collecting a data set specified in the calling parameters.

Within the context above, the TDMS shall include an interpretive System Command Language (SCL) that Authority personnel with appropriate permissions can use to write, execute, modify, debug, and save scripts for different purposes in the form of text listing one or more computer commands. For example, SCL shall allow the user to extract data such as SCADA data points, perform data manipulation using calculation and logic statements, and initiate control actions. A simple example is use of scripts to execute sequential control commands via SCADA. The SCL shall be easy to learn and use without requiring special programming skills. The Contractor's proposal shall have described in detail the capabilities and features of such a command language or equivalent facility as currently offered and/or the specific facility that may need to be developed to meet this requirement.

8.2 Third-Party Software Interfaces

To support the addition of TDMS applications developed in-house or by third-parties, the capability of high-level language programs to access the real-time and relational databases by referencing unique variable names shall be provided. The residency of the referenced variables shall be transparent to the programmer. In addition, the TDMS shall include well-documented non-proprietary APIs that, at no cost and without restriction, may be used by the Authority (or a third-party engaged by the Authority) to develop applications for the TDMS. The APIs and the database documentation shall be sufficient to allow Authority or third-party personnel to integrate the applications independently.

8.3 System Services

The following system services shall be provided for applications that run in the TDMS computing network.

8.3.1 Global Naming Service

Objects of interest in the computing network shall be assigned names in a global directory. Examples of such objects are processors, peripheral devices, and users. The global naming service shall allow users to reference computing network objects in the directory both by name and by type of service.

8.3.2 Network File Service

Services shall be provided to give users access to applicable files in a secure manner. The file system shall provide a reliable, consistent interface that offers the same performance, security, and ease of access for both network and locally resident files.

The network file service shall use the global naming service. It shall allow transparent information access to applications and utilities and shall support functions such as remote copy, backup, and restore across network nodes. It shall be possible to allocate or de-allocate devices to the network file system as well as allocate or de-allocate logical files and their backups to devices via a convenient maintenance procedure. The network file service shall be easily extensible as the TDMS is expanded.

File access shall be restricted by the assignment of user and/or program privileges such as no access, read, write, execute, and combinations of these. Operating system files shall be specifically identified and shall be protected by more restrictive privileges.

Where implemented, network file services shall be restricted to operating only within a component system, e.g., the PDE shall not provide or be given network file system access to the DMZE.

8.3.3 Scheduling Services

Scheduling services shall include a facility for scheduling application activity based on time-of-day, period, and other events. The following shall be provided as a minimum:

1) Triggers shall be definable based on absolute or relative time based on either system or application time.

2) Triggers shall also be definable based on conditions or events raised by any other applications (i.e., based on calls to the scheduling service from applications setting a condition or event).

3) When initiated by this facility, an application shall be provided with a notice that states the reasons for activation (i.e., identification of the trigger).

Scheduling services shall also monitor the correct initiation and completion of periodic applications. These applications shall be monitored for execution at the proper time. The elapsed time shall be governed by a database parameter that is assigned to each application individually. If an application has not completed its execution prior to its next scheduled initiation, the scheduling services shall notify users through appropriate messages. A logging facility shall record statistics on the cycle time and run time of cyclic real-time applications. A simple manual entry shall be provided to turn off the scheduling of each application.

8.3.4 Time Services

The TDMS shall maintain a common system time across all servers, processors, and devices (such as routers, firewalls, and network management devices) and all logging and event archiving systems. The standard used as the primary source of time shall be the data center's already installed time and frequency facility. Provided by the Authority, this facility will determine Universal Coordinated Time (UTC), power system time, time deviation, power system frequency, and power system frequency

deviation. UTC will be obtained from the Global Positioning System (GPS). Thus, TDMS time shall be periodically synchronized to this time standard. Where detected, large deviations shall be annunciated and, upon failure of the time standard, the TDMS shall revert to its own internal time standard.

Application time shall be distinct from TDMS time. Application time shall be shared by a group of applications within a system. Application time shall maintain time and date as understood by the users (e.g., accounting for holidays). It may be driven by TDMS time (the default) or by an application (as in the case of an historical data reconstruction program).

As a minimum, application time services shall support the following features:

1) A uniform internal representation to facilitate normal date and time, relative date and time, arithmetic date and time operations, etc.

2) A date maintenance facility (day in week, date, week number, week in month, day in year, day in month).

3) Support for leap years, unlimited holidays per year, and other critical dates that may be applicable.

4) Ability to define arbitrary time-period types, e.g., area on-peak and off-peak time periods, for use by applications.

8.3.5 Print Services

Hard copy output resources in the computing network, including those outside the TDMS network (such as designated resources on the Corporate WAN), shall be assigned as network (rather than local) resources, and shall be available for use from any node in the network. Users shall be kept informed of the status of their print jobs (e.g., spooled, printed, and completed).

8.3.6 Distributed Backup and Archiving

The TDMS shall include services to back up, archive, and restore all TDMS software and data independently of its location on the TDMS network. Backup shall include TDMS and network configuration information, such as database table and queue sizing, router tables, and firewall access rules. The distributed backup process shall include all procedures and methods including required initial installation media for completely restoring the TDMS from a non-initialized state to a fully functioning state following a hardware disaster for example. A process shall be supplied to test backup media periodically to ensure that the information contained on this media is recoverable if needed.

Once initiated, the distributed backup and archiving services shall automatically back up all information needed to recover from failures or data corruption without manual intervention by users, except for replenishment of removable media. Although the devices being backed up may be physically separate, the backup system shall be managed centrally. The Contractor shall provide options for encrypting, or otherwise securing from disclosure, backup media containing sensitive information.

8.4 Application and System Development

An application, as used herein, shall mean a module of functionality such as data acquisition. An application shall consist of various components such as executable application images, user interface definitions (displays and display interactions), data sets, messages, and reports, all working together to deliver a specific functionality.

8.4.1 Software Configuration Management

An integrated development subsystem supporting C, Java, C++, and other programming languages used in the TDMS shall allow programmers to work together effectively. In this respect, the programming languages C and C++ are preferred.

The Contractor shall provide a software configuration management system to define the elements and associated attributes of an application. Source definitions for the application's elements, the residency requirements (such as local or shared), and any access attributes shall be defined through the software configuration management system.

Source definitions for all elements of an application shall be maintained in files under a code management system. As a minimum, the code management system shall:

1) Manage code and binary images.

2) Allow tracking of code changes by date, author, and purpose.

3) Manage documentation modules and associate them with code, binary images, and other documentation.

4) Support multiple teams of programmers working concurrently on the same modules.

5) Provide an efficient link between modules.

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

8.4.2 Compilers

Compilers with code optimization features shall be provided for all programming languages used in the TDMS. Compilers shall conform to the latest applicable standards (e.g., ANSI and IEEE standards). Program source code shall utilize symbolic interfaces for all application system services. The compiler shall provide extensive error checking facilities, explicit error messages, and complete output listings.

8.4.3 Interactive Debugger

An interactive debugger product shall be supplied that, as a minimum, includes full or selective (interpretative) trace, memory alter and dump, snapshot with or without memory dump, and search

capabilities. The interactive debugger shall utilize symbolic references to statements and variables. It shall also provide simultaneous presentation of the source code with an indication of program flow (i.e., an indicator showing the currently executing statement).

8.5 Diagnostics

The TDMS shall include all diagnostic software provided by the manufacturers of all hardware, including processors and peripheral devices, supplied with the TDMS. The TDMS shall also support error detection and diagnostic tools sufficient to support the requirements of these Technical Specifications. These software tools shall include the capability to automatically monitor the message flows and any communications errors between the TDMS and its field device interfaces, similarly between the TDMS and any other connected system (such as the Authority's GIS), between the TDMS servers at both data centers, and between the TDMS and its remote workstations.

Diagnostics for communications data sources, computer systems, and workstations shall provide at least the following capabilities:

1) Select any communications channel for test.

2) Select a request message for transmission to data sources and computer systems.

3) Select single or cyclic message transmissions to data sources and computer systems for test purposes.

4) Monitor and display information sent to and received from data sources and computer systems.

5) Monitor and display data communication device status.

6) Provide communication statistics including the number of errors, retries, bytes transferred, etc.

The communications diagnostics shall include a "trace" facility for messages as they are sent and received. This facility shall trace all or a selected set of logical channels and shall provide explicit trace information at each level of the protocol stack. It shall be possible to trigger the trace facility manually as well as by program status flags and inter-program messages. The level of detail included in the trace shall be triggered by incoming or outgoing message contents on one or more logical channels, or by any of the methods described.

9. Data Architecture

The database foundation shall include both the schemas (logical descriptions of the databases) and the instances (run time databases) of the real-time, study, simulation, historical, and relational data structures. It shall also encompass all aspects of database management across the distributed architecture of the TDMS.

9.1 General Design Concepts

The data architecture of the TDMS shall include facilities for storage of data defining the state of the power system and the parameters that determine operation of the TDMS. Within this context, as a minimum, the following design concepts shall be applied:

1) High speed access.

2) Secure access from the perspective of preventing:

    a) Unauthorized access (read-only, read-write, create-delete).

    b) Write access by multiple users simultaneously, i.e., ensuring only one user at a time has write access to any single database item.

    c) Storage of invalid data (an appropriate validation scheme is required).

    d) Propagation of corrupted data.

    e) Failures causing permanent loss of critical data.

3) Management of database generations and modifications shall be consistent, easy, modular, and rapid.

4) Management of data exchanges between network nodes, both internally within the TDMS and externally between the TDMS and other systems, shall permit consistent easy modification and expansion of automatic data exchanges and shall keep track of the data with respect to where and when it was transmitted.

5) File systems shall be scalable, i.e., increasing the database size or changing to a large SSD shall not require rebuilding the TDMS or losing data.

6) Modifying portions of the database shall not require the recompilation or re-linking of application software except if the application software has been changed to reflect the database modification.

7) Database redundancy shall be maintained to ensure system availability in the event of hardware or software failure, and all data in the primary and backup database shall be synchronized and consistent.

8) On-line backups of the database shall be permitted in such a way as to not affect on-line operations. It shall not be required to take equipment out of service or perform a failover to back up any component of the system database.

The TDMS database shall make use of templates and other mechanisms to facilitate database generation and maintenance. The user shall interact with the database via a graphical man-machine interface. In addition, the user shall have the capability to interact directly with the database source via

ANSI SQL-compatible queries. Report generation and other non-real-time applications shall also have access to the data via ANSI SQL-compliant calls to any database content.

9.2 Data Access

A library of access routines shall be the preferred means for application programs to interact with the database. This way, application programs (and programmers) only need to concern themselves with the callable Application Interface (API) of these routines. Each application shall interact with the database through the event library. These access routines shall serve as generic APIs for database access thereby eliminating proprietary database function calls at the application level.

Data access shall be supported by the following general capabilities:

1) Interfaces to the database shall be by logical names specified by the Authority. It shall not be necessary for users or applications to have knowledge of the logical or physical structure of the database. TDMS users, including technical staff maintaining the applications or database, shall not be exposed to internal identifiers of database items such as indexes into tables.

2) Application interfaces to the database shall support direct access to the individual elements comprising an entry in the database. Using the analogy of a “table” (as a database) composed of “records” (entries) in turn composed of “fields” (attributes of the entry), the application interfaces shall support read and write access to each of the individual fields without requiring the accessing mechanism to manipulate larger structures such as masking other fields.

3) On-line database browsing and value modification of all database entries by authorized users shall be supported. These users shall be given the capability to sort data for display by various criteria including substation, feeder name, point ID, point name, etc.

4) Automatic propagation of updates and changes to calculated values, by triggering recalculations, shall be provided.

5) Automatic propagation of updates and changes made manually or by program shall take place to all copies of the source database. This process shall be able to handle the situation where added or deleted data causes a shift in the originally assigned locations of data.

6) Physical reconfiguration of the data acquisition and control subsystem shall be transparent to interactive and programmatic database access (e.g., changing the position of a scanned SRTU quantity, or moving it to another SRTU, shall not affect retrieval of that quantity).

7) Multiple concurrent access to the database shall be allowed within the context of support services that provide for deadlock prevention, locking, and access authorization.

8) Transaction monitoring and rollback features shall be provided.

9) Database administration and utility functions, as a minimum, shall include:

    a) Automatic recovery and restart.

b) Triggering of program actions resulting from database updates.

c) Logging facilities to save transactions.

d) Import/export utilities to migrate data to other databases.

e) 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.

10) Distributed database environment shall include:

a) Verification of data integrity.

b) Automatic navigation through the database such that the path used to access the data is transparent to the user, developer, or application program.

9.3 Data Naming

Data items in the TDMS database shall be identified using a consistent naming scheme. Data items representing power system device attributes, including telemetered data and supervisory control outputs, shall accommodate the Authority's existing naming conventions. The existing naming convention, for example, allows for SCADA point names of up to 30 alphanumeric characters and for point descriptions of up to 50 alphanumeric characters. During project implementation, the Authority will provide naming convention details in the form of an applicable template.

9.4 Database Construction and Maintenance

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. Database maintenance refers to the subsequent addition of new database contents and the modification of existing contents. The tools used by the Contractor, such as the TDMS Editor tool (refer to Clause 3.1.3), to construct and maintain the database shall be delivered with the TDMS. The system database shall be documented in a complete database manual that shall be available on-line and that explains the interrelationship of all associated database structures. The database manual shall provide both visual samples and text descriptions of the entry format and purpose of all fields in all such structures.

The TDMS shall include a single logical repository for all data needed to model the real-time, study, simulation, and historical state of the power system and TDMS. All information needed to describe the models (including for example relevant field device I/O points), on which the TDMS operates shall be defined in the database once and once only and made available to all TDMS applications and user interface maintenance tools that need the information. The database shall also include parameters controlling execution of the TDMS functions.

The database shall accept interactive user commands and pre-compiled SQL statements to provide at least the following functions:

1) Storage of the database data definitions, including schemas, relational tables, views, and fields.

2) An active repository component that provides the capability to organize, manage, and control information about users, applications, and programs that access the data.

3) On-line access to review the structure of the database and its data definitions.

4) Development of a new database.

5) Copying of existing database structures.

6) Modification of the database definition without unloading/loading the database.

7) Modifying the existing database, such as adding attributes ("columns" in a table-row-column structure). The addition of attributes shall not disrupt access to existing attributes.

8) Listing of all information on database parameters, attributes, etc.

9) 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.

10) Support for command lists or catalogued procedure input.

11) Automatic time and date stamp on output.

12) Name change utilities that identify all uses of an entity name throughout the TDMS database and facilitate selective and global changes to an entity's name.

13) Processing of the database into the data structures used by the TDMS for on-line applications, i.e., their "run-time" databases.

14) Use of "Global Naming Conventions" with respect to display and database point definitions. This global naming shall provide for unique names throughout the system.

All entries to the database shall be checked for validity. 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 modifications shall be maintained in an audit log. The log shall be displayed and printed on demand.

Data not modified when the 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 the specific items modified. This requirement specifically applies, but is not limited to:

1) Values and attributes of telemetered and calculated points.

2) Models and execution parameters for applications.

3) Save cases.

4) Data that is updated over time, such as averaged data or “smoothed” data.

5) Data entered manually by users.

Modified portions of the TDMS database shall be buffered and shall not be utilized until commanded by a user. A copy of the pre-modification database shall be retained until a subsequent user command indicates that the new database is acceptable. At any time during the "temporary" use of the new database, the user shall be able to command the TDMS to revert to operation using the previous unmodified database. The TDMS shall support multiple files (“work areas”) of in-progress modifications, such that several users can be preparing database modifications at any time.

9.5 Adjustable Parameters

All parameters in the TDMS shall be defined in the database and shall be adjustable by designated personnel. Adjustments made to parameters shall become effective without having to recompile programs or regenerate all or portions of the database. All time periods contained in these Technical Specifications shall be considered initial values for planning purposes, but all software parameters must be adjustable by Authority personnel.

10. Standards

The Contractor shall have identified the standards to which the proposed hardware and software conforms. Where relevant, specific standards including applicable Cyber Security standards are also referenced in these Technical Specifications. From an overall perspective, the design, construction, and performance of all hardware and software supplied by the Contractor shall conform to the latest applicable standards such as those listed hereunder (or equivalent):

1) International Electrotechnical Commission (IEC)

2) International Organization for Standardization (ISO)

3) International Telecommunications Union (ITU)

4) American National Standards Institute (ANSI)

5) Institute of Electrical and Electronic Engineers (IEEE)

6) Electronic Industries Association (EIA)

7) Instrument Society of America (ISA)

8) American National Institute of Standards and Technology (NIST)

9) American National Electrical Manufacturers Association (NEMA)

10) North American Electric Reliability Council (NERC).

The recommendations of the Electric Power Research Institute (EPRI) in the USA regarding preferred suites of standards for electric utility use shall be incorporated where applicable. This includes the recommendations that apply to API support.

Within this context, IEC 61850 is of interest, particularly with respect to potential TDMS use cases that may exploit its GOOSE messaging and Sample Value (SV) features, as in data communications between the TDMS and its FDIs. Consequently, the Contractor's proposal shall have described such uses cases as may apply to the TDMS in the form of options to provide added value for the Authority.

11. Critical Infrastructure Protection

Due to the critical nature of TDMS operations and its networking with other systems, protection against cyber security threats is of major concern to the Authority. While recognizing that such protection is a combination of user security procedures and system security technologies, the TDMS shall incorporate all necessary security system technologies to minimize the possibility of successful security attacks and provide mechanisms for identifying, coping with, and recovering from successful security attacks. The Contractor shall also recommend user security procedures that will make the most effective use of the system security technologies.

Within this context, the TDMS shall be designed using a risk-based approach and applying the principle of defense-in-depth to provide a robust and resilient system, i.e., multiple layers of security controls shall be placed throughout the TDMS such that, in the event a security control fails or a vulnerability is exploited, there is a secondary or redundant control that will prevent, delay, or mitigate the exploit in addition to alerting the Authority so that mitigation steps can be taken.

All security functions must be implemented in a non-interfering manner such that authorized and legitimate use of the TDMS is not hampered, i.e., the ability to perform the required TDMS functions shall not be impeded by the security features. This shall be demonstrated during factory and site acceptance tests during which the TDMS software shall also be audited to ensure that the cyber security measures described in the following sub-clauses and elsewhere in the Technical Specifications are satisfied.

The Contractor shall also provide hardware and software tools by which the Authority can manage the security measures incorporated into the TDMS design. Such tools shall have been described in detail in the Contractor's proposal.

11.1 Applicability of Cyber Security Standards

The TDMS is considered a Critical Cyber Asset. Therefore, notwithstanding any additional cyber security requirements specified herein (also refer to Clause 7), it is preferred that the Contractor's processes and supplied systems conform, as a minimum, to all applicable requirements of the Critical Infrastructure Protection (CIP) standards promulgated by the North American Reliability Council (NERC), including:

1) CIP-002, Critical Cyber Assets.

2) CIP-003, Security Management Controls.

3) CIP-004, Personnel & Training.

4) CIP-005, Electronic Security.

5) CIP-006, Physical Security.

6) CIP-007, Systems Security Management.

7) CIP-008, Incident Reporting and Response Planning.

8) CIP-009, Recovery Planning.

As applicable, the Contractor's security measures shall also comply with other cyber security standards and guidelines such as:

1) ISO/IEC 27002/27019, Information technology – Security techniques – Code of practice for information security management.

2) NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security.

3) IEC 62433, Industrial communication networks – Network and system security.

4) IEC 62351 series of Cyber Security standards as applicable to the TDMS communication protocols that include:

    a) Secure ICCP based on IEC 60870-6-TASE.2 to provide a secure exchange of information between the TDMS and the EGAT SCADA/EMS for example.

    b) IEEE 1815-2012 (secure DNP 3.0) to provide secure exchanges of telemetry and control between the TDMS and its FDIs.

    c) IEC 61968 and IEC 61970 to provide XML exchanges of data in the form of Common Information Model (CIM) profiles between the TDMS and other systems.

    d) IEC 61850 to provide (as an option for possible future use) secure exchanges of telemetry and control between the TDMS and its FDIs.

5) BDEW white paper, Requirements for Secure Control and Telecommunication Systems.

Which security standards are incorporated in the TDMS, and where and how they are incorporated, shall have been described in detail in the Contractor's proposal.

11.2 Security Awareness Program

The Contractor shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall cover the policies, access controls, and procedures developed for Critical Cyber Assets and include, as a minimum, the following required items appropriate to personnel roles and responsibilities:

1) The proper use of Critical Cyber Assets.

2) Physical and electronic access controls to Critical Cyber Assets.

3) The proper handling of Critical Cyber Asset information.

Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a cyber security incident.

In addition, the Contractor shall conduct the Cyber Security Measures training course as described in Clause 23.4.5.

11.3 Firewall Protection

The Contractor shall design TDMS security zones by using appropriate firewall devices. Firewalls shall limit access at the packet and application levels. Each firewall shall support the following features:

1) **Authentication** – The firewall shall require authentication of users and software applications as they exchange data through the firewall.

2) **Access Control** – The firewall shall provide access control through Access Control Lists (ACLs) and through limiting the number of open ports to only those required for TDMS operation. Changes to ACLs shall only be implemented via authorized and authenticated means and shall be logged.

3) **IP Spoofing** – The firewall shall guard against IP spoofing by using authentication access control validation of IP addresses.

4) **Packet Filtering** – The firewall shall implement filtering of both inbound and outbound traffic and shall restrict access based on both source and destination IP addresses.

5) **Reject Unauthorized Traffic** – The firewall shall reject packets originating from outside the local network that claim to originate from within.

6) **Prevention of Denial of Service** – The firewall shall protect against denial of service attacks by rapidly rejecting unauthorized packets that may overwhelm a port. The Contractor's proposal shall have described which types of denial of service attacks the firewall can prevent.

7) **Network Address Translation** – The firewall shall perform Network Address Translation (NAT) to permit the Authority to hide the IP addresses used on the internal TDMS network from external view.

The Contractor shall be responsible for the configuration of the firewall with Authority assistance to define the access rules. The following general access rules shall be implemented:

1) Access from the TDMS to systems on the Corporate or any other security network shall be allowed only via a DMZ.

2) Access to the TDMS from users and systems on the TDMS security network shall be limited by IP address and user (or account) name.

3) Only selected users at selected nodes (IP addresses) shall be permitted access to the IS&R databases. The access control facilities of the IS&R will be used to further limit access.

4) Only selected users at selected nodes shall be permitted access to the TDMS for TDMS user interface functions.

The Contractor shall deliver protocol analyzer and sniffer software for the local and wide-area networks of the TDMS. This software shall be compatible with the TDMS communications equipment and shall be installed in portable Contractor-provided test sets, referred to as Network Test Sets (NTSs), in the form of notebook PCs.

11.4 Removal of Unused Services

All applications, utilities, system services, scripts, configuration files, databases, user accounts, and all other software not required for operation of the TDMS shall be removed prior to commissioning. The items to be removed shall specifically include, but not be limited to:

1) Games.

2) Device drivers for devices not delivered.

3) Servers and clients for unused Internet services.

4) All software compilers except for the PPE.

5) Software compilers for languages that are not used in the TDMS.

6) All unused protocol suites.

7) Unused administrative utilities, diagnostics, network management, and system management functions.

8) Backups of files, databases, and programs, used during system development.

9) Databases, configuration files, and other files used for development and testing.

10) Programs and scripts used for development and testing including sample programs and scripts.

11) All text as may be in the system for Contractor development purposes. For example, system displays, databases, and logs shall not contain such text.

12) Help systems not directly supporting TDMS applications.

Preference shall be given to the supply of additional “hardening” following established methods and guidelines including, but not limited, to those developed by the original software vendor as well as the

US Government National Institute of Standards and Technology, Department of Defence, and Department of Energy, or similar recognized organizations.

11.5 Software Updates and Virus Scan

All patches and upgrades to the operating system and applications software shall be tested and certified by the Contractor. Thus, whenever the Contractor or suppliers of software to the Contractor release a software change ("upgrade", "update", "modification", "release", or "patch"), including correction to a security-related error in the code or closure of a known vulnerability, the Contractor shall take immediate steps to test, confirm, and install the software change on the TDMS.

The software shall be scanned for viruses, worms, Trojan horses, and other software contaminants during the TDMS factory and site tests.

11.6 Free of "Electronic Self-Help" Enabled Software

The TDMS software shall not contain embedded faults or back-door mechanisms that allow the Contractor or any other party to remotely disable some or all software functions, affect their performance, or in any way degrade its operation (so-called "*electronic self-help*" in the terms of the Uniform Computer Information Transactions Act). The software shall not contain any mechanism that automatically disables some or all functions or degrades their operation on a certain date or upon the occurrence of a specific event.

11.7 Detection of Unauthorized Modifications to Software

The Contractor shall provide a mechanism for periodically scanning the integrity of the software on the TDMS to determine if unauthorized modifications to the software have been made. A tool, such as Tripwire[2] or equivalent, may be used for this function. The process of making an authorized modification to the software shall include an update to the integrity database to ensure that the scanning tool does not detect valid or authorized changes as unauthorized. The scanning software shall be configurable to run manually or periodically and shall not interfere with the performance or operation of the TDMS or any application.

11.8 Anti-Virus and Malware Detection Software

The Contractor shall implement anti-virus, spyware, and other malware detection systems. These systems, using commercially available products where possible, shall be installed and running throughout the development, test, commissioning, and acceptance of the TDMS to ensure that the impact of these systems on TDMS performance is known and tested. The Contractor shall provide procedures for the secure updating of configuration and signature files to ensure that the tools remain current with updates and releases.

[2] *Tripwire is a trademark of Beldem, Inc.*

11.9 Security Monitoring and Reporting

The TDMS shall log all access attempts at both the application and electronic security perimeter. The TDMS shall maintain logs of system events related to security in sufficient detail to create historical audit trails and enable a root-cause analysis for a period of at least 90 calendar days. If required, it shall be possible to copy the system event data to an alternative storage medium as part of an investigation covering more than 90 days. As a minimum, the logs shall capture the following user access requests:

1) All attempts to log on, both successful and unsuccessful.

2) Any privilege change requests, both successful and unsuccessful.

3) All user actions affecting security, such as changing passwords.

4) All attempts to access files for which the user has no access privileges.

5) Attempts to perform an action not authorized by the security scheme.

6) Detecting unauthorized access (intrusions) and attempts at unauthorized access at the access points to electronic security perimeters twenty-four hours a day, seven days a week.

For the purposes of the above requirements, the term “user” shall refer both to human users and to applications requesting such actions.

All access records shall be stored within the TDMS on auxiliary memory. The format of these records shall be consistent with those provided by other log generating devices, such as network routers, firewalls, and intrusion detection systems. 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. Access recording shall include a feature to archive the record file and to direct the records to a new empty file.

The TDMS shall generate an alarm when access activity may be indicative of attempts to obtain unauthorized access to system services or data. A simple method shall be provided for the user to view and to change the rules for generating alarms. Initially, an alarm shall be generated when the system detects any of following activities:

1) Repeated attempts from a specific workstation or external port to log in.

2) Repeated failed attempts at file access.

3) Port scans (attempts to access closed ports or services).

4) Unusual levels of traffic on the local area network.

11.10 Generic and Default Accounts

The Contractor 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 contractors. Where specific accounts cannot be removed, they shall be renamed or disabled to prevent unauthorized access.

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. This action provides both authentication of a specifically named, valid user, as well as an audit trail of any elevated privilege actions performed.

11.11 Account Management

Account management shall include software used to access directories containing critical information such as user names and authentication information, addresses, access control lists, and cryptographic certificates. Such software based, for example, on Version 3 of the Lightweight Directory Access Protocol (LDAP) may be provided. Applicable protocol certification, as required by the delivered TDMS, shall be provided by the Contractor. How future upgrades and certifications may be attained shall have been described in the Contractor's proposal. This shall be possible without Authority dependence on the Contractor.

11.11.1 Role-Based Access Control

The Contractor shall implement Role-Based Access Control (RBAC) in compliance with IEC 62351-8. Users shall have individual user accounts, whereas roles shall be assigned to functional accounts with established rights and constraints. Software applications that are used to interact with the TDMS shall also be considered as RBAC "users".

Default roles/functional accounts shall be provided for basic operational and engineering activities, including security management, with default privileges assigned down to the individual device and type of data. These default roles and their privileges shall be modifiable.

No user shall be able to access the TDMS without having their user account assigned to at least one role. That role shall determine what access privileges the user has.

The Contractor shall provide for user accounts with configurable access and permissions associated with the defined user role and shall provide a mechanism for changing user-to-role associations.

The Contractor shall adhere to least-privilege permission schemes for all user accounts, and application-to-application communications.

The Contractor shall configure the system so that initiated communications shall start with the most privileged application controlling the communication. Upon failed communication, the most privileged side will restart communications.

The Contractor shall ensure that under no circumstances can a user escalate their privileges without logging into a security management role first.

11.11.2 User Account Password/Authentication Management

A centralized mechanism for defining and controlling user access to the operating system environment of the TDMS shall be provided. For example, as referenced elsewhere in these Technical Specifications, a two-factor authentication procedure shall apply for dispatcher and data engineering users. The TDMS must support account management methods to enforce access authentication and accountability of user activity and to minimize the risk of unauthorized access. The TDMS and the underlying operating system must support the requirement that users have individual accounts without compromising the functionality and operating restrictions. Where individual computer nodes maintain their own unique internal user identification codes, the same named user shall use the same internal user identification code for all nodes

The Contractor shall provide a configurable user account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of login attempts, inactive session logout, screen lock by application, and denial of repeated or recycled use of the same password. Passwords shall not be stored electronically or in Contractor supplied hardcopy documentation in clear text unless the media is physically protected. The configuration interface to the account management system shall have controlled access.

The Contractor shall provide a mechanism for rollback of security authentication policies during emergency system recovery or other abnormal operations, where system availability would be negatively affected by normal security procedures.

All accounts in the delivered TDMS shall use passwords assigned by the Authority. Passwords for maintenance access shall be constructed to maximize the amount of computer processing required to guess the password.

All accounts providing interactive or network access shall have passwords. Accounts that exist strictly for identification and ownership purposes shall be disabled from all interactive, network, or other access within the TDMS.

11.11.3 Account Audit and Logging

The Contractor’s centralized account management system shall include the logging of user and functional account activity that is also auditable both from a management (policy) and operational (account use activity) perspective. The audit trails and logging files shall be time stamped, encrypted, and access controlled.

11.12 Appropriate Use Banner

Users accessing the TDMS through interactive or maintenance access shall be presented with an “Appropriate Use Banner” on the user screen upon all access attempts, the contents of which will be provided by the Authority.

11.13 Secure Maintenance Access

Secure maintenance access to the operating environment shall be provided for both remote and local users. The access shall provide authentication of valid users without transmitting plain-text passwords on the network. An encrypted access mechanism such as Secure Shell (SSH) shall be used for "command line" access. Secure file copy features included in SSH shall be used to manually transmit files between nodes when using the network.

11.14 Authorization Process for Contractor Personnel

The Contractor shall use a secure authorization process to grant Contractor personnel access to the TDMS while on site at the Contractor's development site. Additionally, the Contractor shall continue to use the authorization process in the field during site start-up, commissioning, and ongoing maintenance of the TDMS.

The Contractor shall maintain lists of all authorized personnel with access to the TDMS while on site at the Contractor's development site, including their specific electronic and physical rights to the systems, processors, or databases, and a date for which access will be terminated. The Authority shall be informed of all changes to the list.

11.15 Session Management

Users shall be required to login to one of their assigned role-based functional accounts to start a session.

The Contractor shall not permit user login credentials to be transmitted in clear text. The Contractor shall provide the strongest encryption method commensurate with the technology platform and response time constraints.

In addition, where appropriate, the Contractor shall not allow the same user to log in to multiple accounts concurrently, nor for applications to retain login information between sessions, nor provide any auto-fill functionality during login, nor allow anonymous logins.

The Contractor shall provide user account-based logout and timeout settings for all administrative accounts.

11.16 Hardware Configuration Protection

The Contractor shall disable, through software or physical disconnection, all unneeded communication ports and removable media drives, or provide engineered barriers.

Where appropriate, the Contractor shall configure the network devices to limit access to/from specific locations. All configuration changes shall be validated and logged.

The Contractor shall configure the system to allow the system administrators the ability to re-enable devices if they are disabled by software.

The Contractor shall provide network and system management for monitoring the health of the networks and systems. The Simple Network Management Protocol (SNMP v3, IETF RFC 3411–RFC 3418) shall be used for common network devices such as routers and firewalls. IEC 62351-7, which defines additional power system-specific Management Information Base (MIB) objects, shall be used for monitoring other types of systems and equipment.

The Contractor shall identify heartbeat signals or protocols and recommend whether they should be included in network monitoring. If they are to be included in network monitoring, the Contractor shall provide packet definitions of the heartbeat signals and examples of the heartbeat traffic.

11.17 Security Patch Management

The Contractor shall have a patch management and update process for operating systems, applications, and third-party software. The Contractor's proposal shall have provided details of the patch management and update process including the procedures for the installation and update of patches.

Within this context, the Contractor shall notify the Authority of known vulnerabilities affecting Contractor-supplied or required OS, application, and third-party software. Notification shall be sent to the Authority within 48 hours of the vulnerabilities becoming known. Notification of associated security patches shall also be provided.

The Contractor shall apply, test, and validate patches on a baseline reference system before distribution. A baseline reference system is an instance of the Contractor's base software product without any customization that is used for release and patch management testing. This baseline reference system shall be a Contractor internal system. Testing shall have the goal of confirming that the patch does not introduce any new errors and does not interfere with the TDMS. The security patch shall be tested and sent to the Authority by the Contractor in a secure fashion within 7 (seven) days of its release.

The Authority will test the patches in the PPE to simulate an operational environment. Testing and installation of all security patches shall follow a Contractor-established configuration management and change control process. This includes the execution of test procedures where the change is deemed "significant."

If during testing in the PPE, a patch is found to interfere with the operation of the TDMS software, the Authority will notify the Contractor and the Contractor shall initiate a resolution procedure.

Notification and closure of security-related vulnerabilities shall be taken as a Contractor obligation throughout project implementation and shall remain as such during warranty and for the time a TDMS service agreement is in place.

After warranty, without a service agreement, the Contractor shall also notify the Authority of security-related vulnerabilities. Closure of security-related vulnerabilities in the absence of a service agreement will be handled on an individual contract basis.

The Contractor shall provide the Authority with a process to submit problem reports as part of the system security process. Submitted reports shall be reviewed and an initial action plan generated within 48 (forty-eight) hours of submittal.

The Contractor shall protect problem reports of a security nature from public disclosure and when notifying other customers shall not release any information to indicate that the Authority identified the problem.

The Contractor shall verify and provide documentation that all TDMS processes are patched to the appropriate currently known security status.

11.18 Web-Based Interfaces

The Contractor shall remove or disable all software components and services that are not required for the operation and maintenance of the devices that run secure HTTP (HTTPS) servers and shall provide documentation on what is removed and/or disabled.

The Contractor 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 Web applications and servers and maintain the established level of system security.

The Contractor's proposal shall have provided documentation on the actual process used for verification and validation of Web-based interface software.

The Contractor shall follow secure coding practices and reporting for all Web-based interface software. This requirement includes both Web applications and servers. Based on risk analysis, the Web applications shall be protected using best practices.

11.19 Recovery Plans for Critical Assets

Bare metal recovery is a technique for the recovery and restoration of a computer without the need to install previously existing software or OS. Examples of this are the Linux DD utility that can copy file systems between disk images and partitions of equal or larger sizes, the Microsoft Windows recovery environment, and several third-party suppliers of similar software.

The Contractor shall provide a comprehensive procedure for the restoration of all hardware, software and configuration such that a "bare metal" rebuild can be achieved. This procedure and the time to complete a "bare metal" build shall have been described in the Contractor's proposal.

12. System Interoperability

The objective of the TDMS capability requirements from an interoperability perspective is to enable the TDMS to automate data exchanges with other Authority IT/OT systems and applications that exist or will exist in the foreseeable future. These include systems such as the Geographic Information System (GIS), Meter Data Management System (MDMS), Outage Management System (OMS), and Asset Management System (AMS), and the application suite comprising DigSILENT. The MDMS represents an aggregation system associated with one or more Advanced Metering Infrastructure (AMI) head-end systems.

Thus, to the extent possible, the TDMS shall be delivered in a form that is system integration ready from the perspective of the Authority's Smart Grid initiatives and Enterprise Application Integration (EAI) plans. Within this context, the TDMS as a minimum shall support the system interoperability requirements as specified herein.

12.1 Background

Exhibit 12-1 identifies the systems and application (collectively referred to as the in-scope actors) that, in addition to the TDMS, are associated with an anticipated future state of the Authority's OT/IT environment. These in-scope actors are required to exchange data with the TDMS.

They are used to identify a conceptual architecture, i.e., an architecture vision, which focuses on TDMS integration with Authority existing and/or future enterprise systems. The resulting architecture, identified in Exhibit 12-2, is based on a logical representation of the systems to be integrated, but does not necessarily align with the physical systems that are used or will be used to host the applications. Exhibit 12-2 also identifies other systems or actors that may need to be integrated at some time in the future but, for now, are considered out-of-scope.

To facilitate events and data exchanges with other systems, the TDMS shall be required to provide the interfaces/endpoints as illustrated in Exhibit 12-3. The Contractor shall work closely with the Authority to identify the data comprising these interfaces/endpoints in detail during project implementation.

12.2 Interoperability Gateway

The TDMS shall have an interoperability gateway to enable implementation of manageable, secure, and auditable two-way communications channels over the networks between the TDMS and other Authority OT/IT systems and applications.

For example, as in Exhibit 12-3, the gateway in the form of middleware shall provide in effect a demilitarized zone between the TDMS and an Enterprise Service Bus (ESB). The ESB will be provided by the Authority.

Thus, the interoperability gateway shall:

1) Allow the TDMS to provide or consume services to or from external systems and applications.

2) Allow the TDMS to provide or consume data via Message Queues, e.g., Java Message Service (JMS).

3) Allow staging tables to be created by which the TDMS can write or read data either consumed or provided by external systems and/or applications.

Exhibit 12-1: System Integration In-Scope Actors

ID	Actor	Actor Type	Description
1	TDMS (PDE, PPE)	System	To monitor and control the power system, the PDE collects data from IEDs and, as may be necessary, sends commands to

ID	Actor	Actor Type	Description
			these IEDs (e.g., SRTUs and FDIs). It includes the TDMS applications that use this data, which is augmented by dispatcher input and calculated values. The PPE uses data from the GIS to create and manage the static network operations model and associated user-interface displays. As a pre-production version of the PDE, the PPE can also collect data and send commands for test purposes.
2	TDMS (DMZE)	System	The DMZE stores or provides real-time and other data received from the TDMS so it can be viewed by dispatchers and other users (both OT and IT personnel), in reports or dashboards, and/or used for analysis. It also receives or stores data from external systems that the TDMS requires. For example, the DMZE supports secure TDMS interoperations with the Authority's OMS and MDMS (i.e., the Authority's AMI facilities) and data exchange with EGAT's EMS.
3	Outage Management System (OMS)	System	The OMS accepts trouble call information from the Authority's Customer Information System (CIS) and generates outage information that can be used to initiate work for power system troubleshooting and repair and, subsequently, to provide customers with estimated power restoration times. It expedites fault location based on not only customer call-in information and the use of dynamic LV connectivity models, but also data made available from Authority AMI facilities.
4	Geographical Information System (GIS)	System	The GIS manages geographical, attribute, and circuit connectivity information that corresponds to the Authority's electrical transmission and distribution assets. In this respect, it is a source of data used by the TDMS and OMS.
5	Meter Data Management System (MDMS	System	The MDMS collects, persists, validates, estimates, and permits editing of customer metering data that can be made available to authorized systems such as the TDMS and OMS as well as Billing. In this respect, it acts as a gateway to AMI Head-End Systems (HESs) for near real-time access to customer metering data.
6	Asset Management System (AMS)	System	The AMS, as a future system, collects information from various sources, such as the TDMS, to support Authority asset management services. For example, it collects asset status and health information that can serve a condition-based maintenance program.
7	DigSILENT	Application	DigSILENT includes a suite of off-line power system analysis software for Authority study and planning purposes related to electrical power transmission and distribution networks. Thus, the TDMS is a source of data for DigSILENT, e.g., a source of save cases for off-line study, where a save case provides not only the applicable network model data, but also the electrical state of the network.
8	ERP	System	Enterprise Resource Planning (e.g., SAP) is a source of information for the TDMS.
9	Business Intelligence (BI)	System	Business Intelligence, e.g., analysis and reporting based on Operational Data Warehouse information. In this respect, the TDMS is a source for such information.

4) Allow the TDMS to provide or consume services to or from external systems and applications.

5) Allow the TDMS to provide or consume data via Message Queues, e.g., Java Message Service (JMS).

6) Allow staging tables to be created by which the TDMS can write or read data either consumed or provided by external systems and/or applications.

7) Allow folders to be created by which the TDMS can share Flat Files with external systems and/or applications.

8) Allow any combination of the above mechanisms to be used.

Exhibit 12-2: SG Logical Architecture Vision (TDMS Interoperability Perspective)

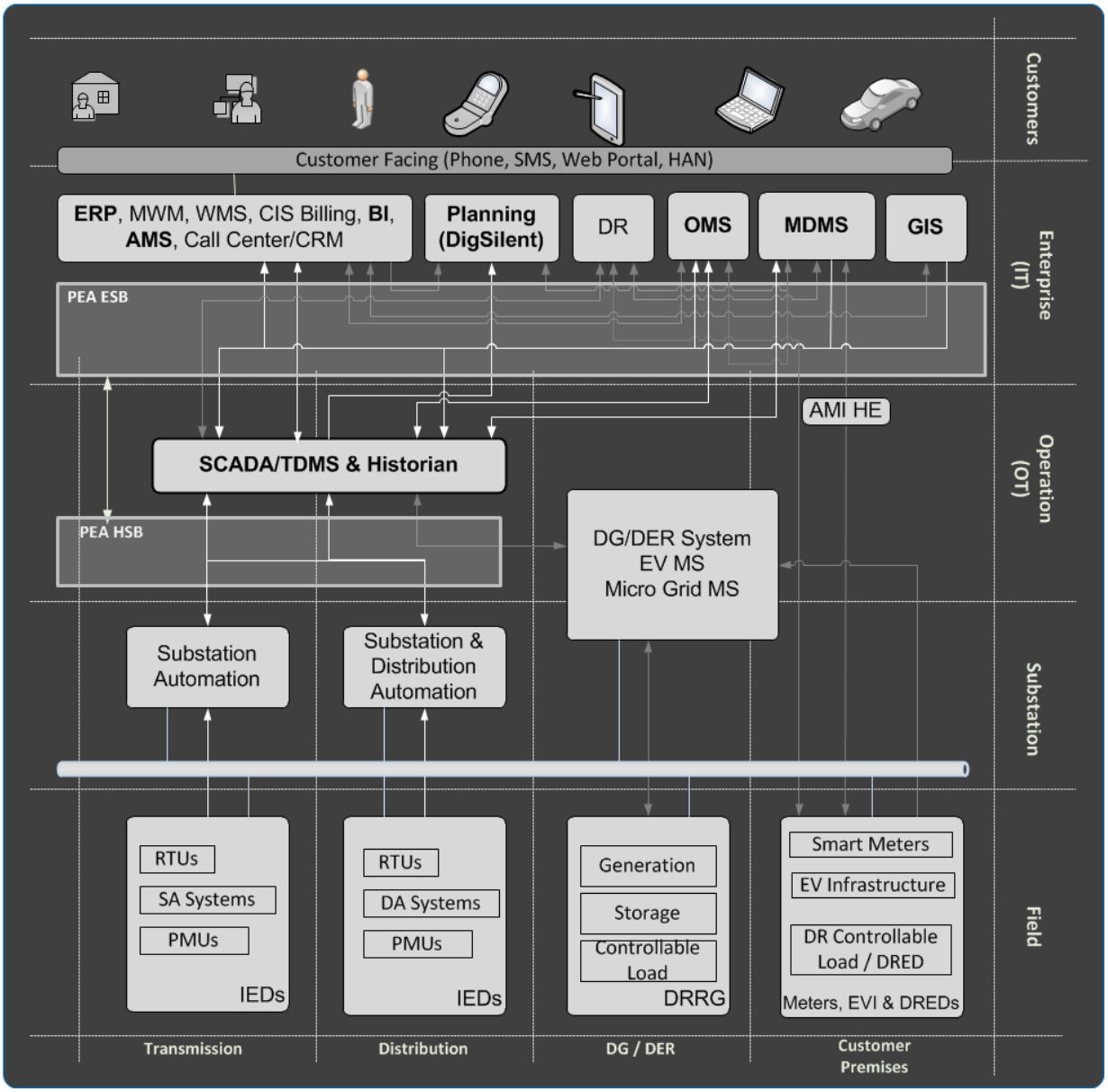
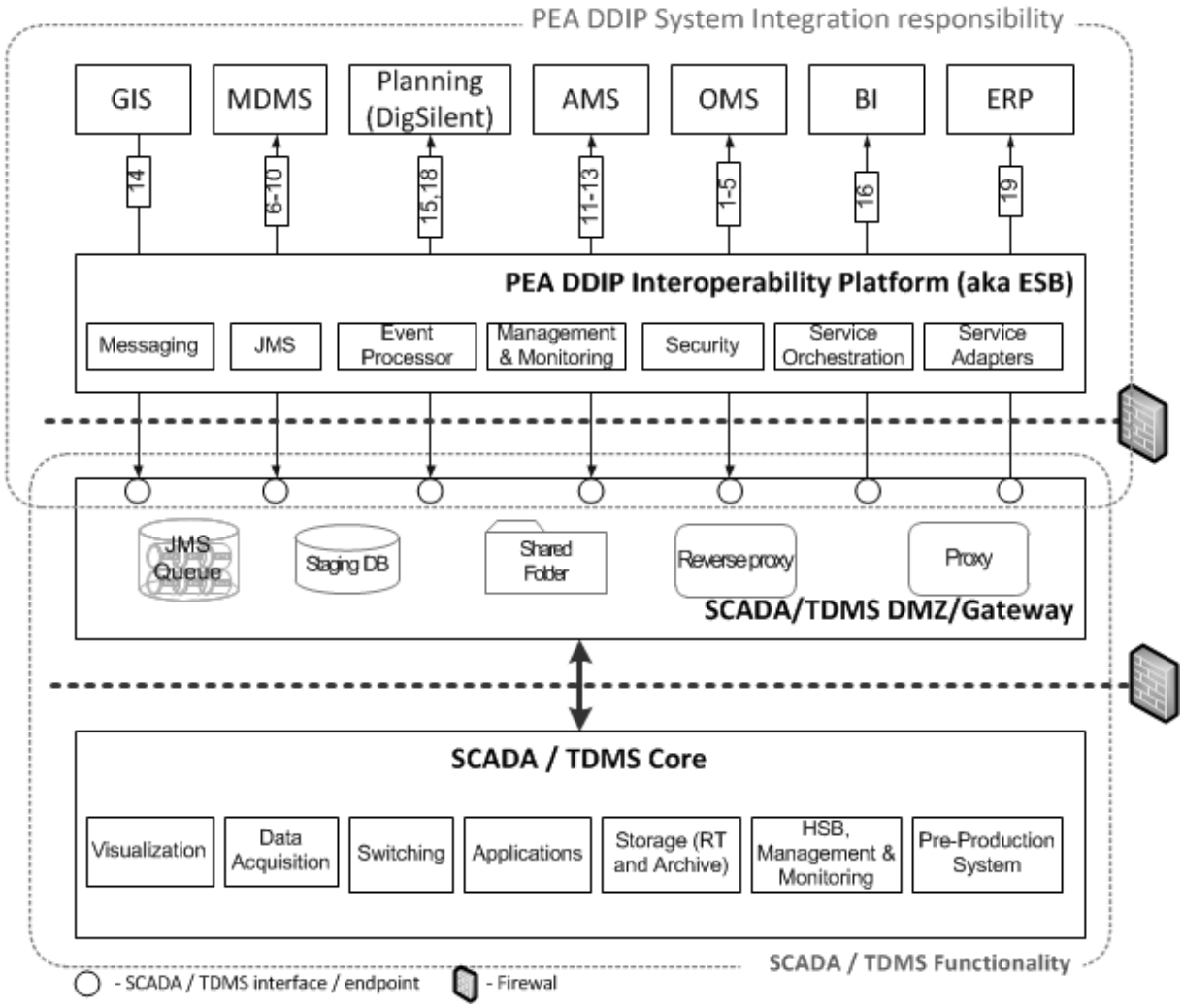


Exhibit 12-3: SCADA / TDMS Integration Scope and Responsibility Diagram



12.3 Role of Common Information Exchange Semantic Model

One of the key elements of the interoperability approach is to establish an Authority, common information exchange, Semantic Model where various applicable industry standards are leveraged as reference models.

To generate the data model and subsequent implementation artifacts and meet the requirements for semantic consistency across systems and data stores that interact with the TDMS, the data modeling process requires the Contractor to describe information exchanges at data element level in a semantically unambiguous way. Such descriptions shall be provided in CIM-like UML diagrams or in spreadsheet formats. A common semantic understanding is essential as a vehicle for streamlining integration activities.

12.4 TDMS Interface/Data Exchange Specifications

Functionally, via a comprehensive integration infrastructure supporting applicable industry standards, the TDMS shall support data exchanges with other OT/IT systems as listed in Exhibit 12-4, i.e., the TDMS shall provide integration ready services and end points designed to support the flow of data from a source of data to a target for receiving the data.

In this respect, for each data flow, Exhibit 12-4:

1) Identifies the provider or source of data.

2) Identifies the system or application that is the target for receiving and consuming the data.

3) Provides a description of the data being exchanged.

4) Indicates how the flow of data may be triggered, e.g., periodically at a specified frequency, on demand, or when a specified event occurs.

5) Indicates the candidate data flow standards that are applicable.

Exhibit 12-4: TDMS Data Exchanges

ID	From / Source	To / Target	Description	Frequency / Trigger	Applicable Standard
1	TDMS	OMS	• Switching Status (change of status such as switching action) • Telemetered and Calculated Analog values consisting of predefined data points such as certain voltages and currents that are required by the OMS (report-by-exception) • Outage Alarms and Events • High Priority Non-Outage Alarms (e.g., transformer winding temperature alarms, substation intruder alarms, low SF_6 gas alarms, etc.)	Event Driven / On occurrence	IEC 61968 MultiSpeak AI 2.5, 6.4
2	TDMS	OMS	• Planned Outages (lines, transformers, cables) • Unplanned Outages	Event Driven / On occurrence	IEC 61968 MultiSpeak AI 2.5, 6.4
3	TDMS	OMS	• Planned Outage Switching Orders – Identification number – Authorization number – Work order number – Current state (undefined, proposed, scheduled, prepared, checked, authorized, rejected, postponed, active, on-hold, terminated, completed, and archived) – Title – Author – Type of work – Description of work – Location of work – Forward/reverse switching scheduled time – References to related switching orders	Event Driven / On occurrence	IEC 61968 MultiSpeak AI 2.5, 6.4

ID	From / Source	To / Target	Description	Frequency / Trigger	Applicable Standard
			– History log – List of switching items		
4	TDMS	OMS	• Temporary Network Changes (cuts, jumpers, grounds)	Event Driven / On occurrence	IEC 61968 MultiSpeak AI 2.5, 6.4
5	OMS	TDMS	• Predicted and Reported Outages	Event Driven / On occurrence	IEC 61968 MultiSpeak AI 7.2, 7.5
6	TDMS	MDMS	• Meter Read Requests such as: – Voltage / Loading – Power Factor – kWh, kVarh – kW, kVar	Event Driven /Request	IEC 61968-9 MultiSpeak AI 2.1, 6.3
7	MDMS	TDMS	• Meter Read Replies such as: – Voltage / Loading – Power Factor – kWh, KVarh – kW, kVar	Event Driven / Reply	IEC 61968-9 MultiSpeak AI 3.2, 3.5
8	MDMS	TDMS	• Sampled Measurement Values	15 minutes / Task / Time Scheduler	IEC 61968-9 MultiSpeak AI 3.2, 3.5
9	MDMS	TDMS	• Meter Events – Power Quality Alarms (sags, swells, etc.) – Voltage Loss Alarms – Reverse Power Flow Alarms – Timestamp	Event Driven / On occurrence	IEC 61968-9 MultiSpeak AI 3.2, 3.5
10	TDMS	MDMS	• Load Profile Requests	On demand	IEC 61968-9 MultiSpeak AI 3.2, 3.5
11	MDMS	TDMS	• Load Profiles	On demand	IEC 61968-9 MultiSpeak AI 3.2, 3.5
12	TDMS	AMS	• Measurements, Status Indications, Alarms, and Events such as: – RCS gas leaks – Overloads – Battery alarms – Communication equipment failures – AC failure alarms – RTU/transformer temperature – Number of breaker trips – Number of switch operations	Daily feeds / Task / Time Scheduler	IEC 61968-4 MultiSpeak
13	AMS	TDMS	• Asset Health Condition • Failure Risk	Daily feeds / Task / Time Scheduler	IEC 61968-4 MultiSpeak
14	AMS	TDMS	• Line, Cable, Transformer Outages	Daily feeds / Time Scheduler	IEC 61968 MultiSpeak
15	GIS	TDMS	• Geographical Power System Network information (as-built) • Bulk and Incremental Updates	Periodic feeds (daily, weekly,	IEC CDPSM 61968-13 Open

ID	From / Source	To / Target	Description	Frequency / Trigger	Applicable Standard
			– Network connectivity – Device information – Electrical location (coordinates) – Element names including, for example, substations, buses, lines, transformers, circuit breakers, and loads – All required attributes associated with elements or objects such as impedance, line length, etc. – Normal status of switches including circuit breakers and disconnects – Geographical information such as physical location of substations, feeder poles, feeder sections, power apparatus (including distribution transformers), field equipment, etc.	monthly) / Task / Time Scheduler	Geospatial Consortium Geography Markup Language (GML) KML Multispeak AI 9.1, 9.3
16	TDMS	Planning DigSILENT	• Snapshot of power system network's dynamic status in IEC CIM format	On demand	61968-6 MultiSpeak AI 2.3
17	TDMS (DMZE)	DigSILENT	• TDMS Data – Measurement reads (loading and power quality) – Switching status – Alarms and events	Daily feeds / Task / Time Scheduler	IEC 61968-6 MultiSpeak AI 2.3
18	DigSILENT	TDMS	• Planned Outages	On demand	IEC 61968-6 MultiSpeak AI 5.2
19	ERP	TDMS	• Notice of Defect (NOD)/outage labels to appear on TDMS displays • Equipment electrical parameters/specifications data	On demand	IEC 61968 MultiSpeak
20	TDMS (DMZE)	BI	• TDMS Data – Outage statistics – Measurement values – Switching status – Alarms and events	Daily feeds / Task / Time Scheduler	IEC 61968 MultiSpeak AI 2.3

Another view of the required or potential TDMS data exchanges is shown in Exhibit 12-5 where a summary of the data exchanges at the entity level represents a TDMS interface/endpoint matrix that identifies which of the interoperability actors provide data and which of them consume data. A corresponding TDMS data exchange diagram is also presented in Exhibit 12-6.

These exhibits, including Exhibit 12-1, Exhibit 12-3, and Exhibit 12-4, are not necessarily complete, but are used as a provisional illustration of the Contractor's scope of work as it pertains to TDMS interoperability with the Authority's other OT/IT systems. Further details shall be resolved during project implementation.

Exhibit 12-5: TDMS Interface/Endpoint Matrix

Description	System							
Data Exchanges at Entity Level **P - Data Provider** **C - Data Consumer**	**TDMS**	**MDMS**	**GIS**	**OMS**	**AMS**	**BI**	**ERP**	**DigSILENT**
Meter Events	C	P						
Meter Reads	C	P						
Load Profiles	C	P						
Sampled Measurement Values	C	P						
Planned Outage Switching Orders	P			C				
Temporary Network Changes (Cuts, Jumpers, Grounds)	P			C				
Predicted and Reported Outages	P			C				
Planned Outages	C				P			P
Geographical Distribution Network Information (As-Built Network Model)	C		P					
Health, Condition, Failure Risk	C				P			
Equipment Electrical Parameters/Specifications Data	C						P	
TDMS Measurement Status, Alarms, and Events	P			C	C	C		C
Snapshot of Distribution Network Dynamic Status in IEC CIM format	P							C

It is within this context that the Contractor shall have proposed an approach to interoperability that shall result in:

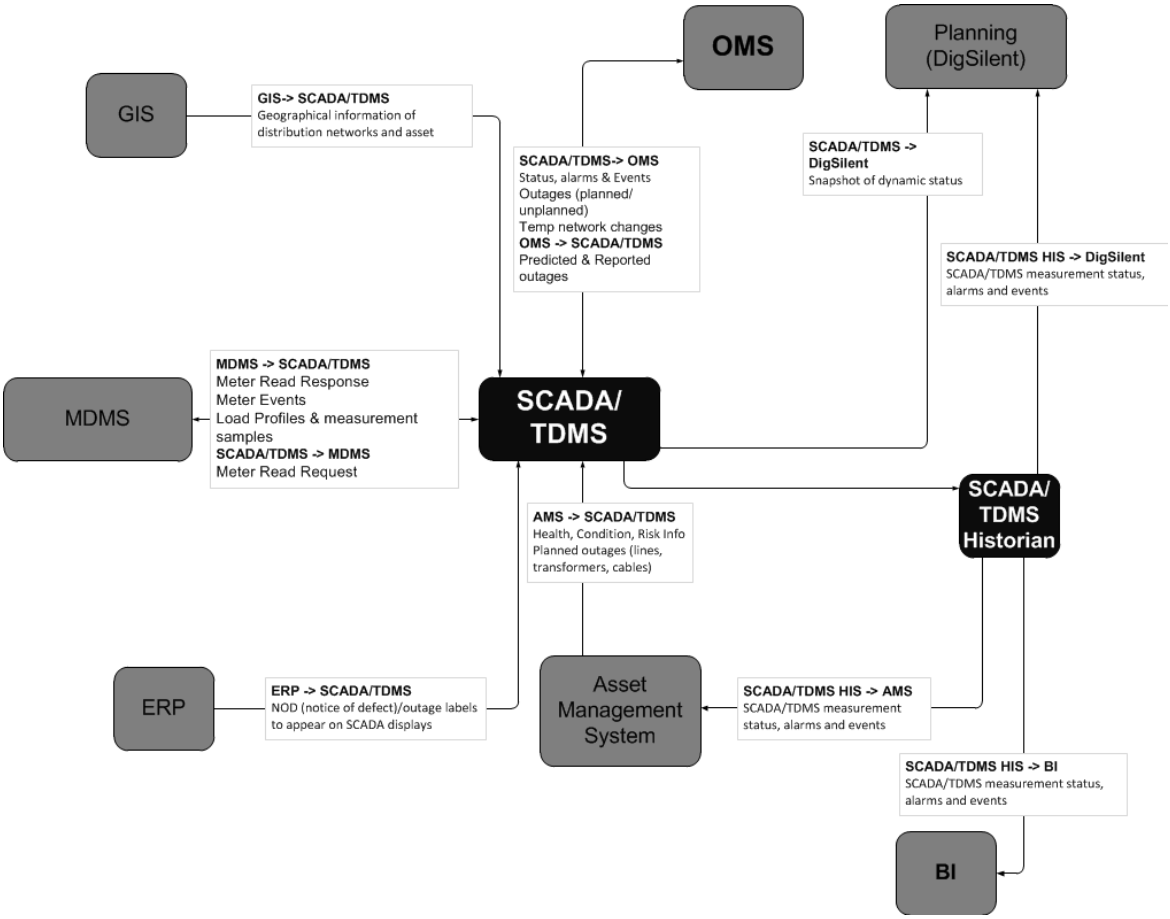
1) Implementation of TDMS data exchanges such as those in Exhibit 12-4 mediated by an integration platform provided by the Contractor.

2) Implementation of the data exchanges using an automated point-to-point integration method.

3) Manual data exchanges if, for example, an Authority integration infrastructure (e.g., an ESB suite) is not available or not ready to facilitate automated data exchanges with the TDMS. In addition, if the point-to-point method cannot be automated.

4) As may be necessary, implementation of such TDMS data exchanges by using any combination of the above mechanisms.

Exhibit 12-6: TDMS Data Exchange Diagram



13. Early Development and Quality Assurance Systems

As components of the TDMS Pre-Production Environment (PPE), the Contractor shall deliver early forms of the Development System (DVS) and Quality Assurance System (QAS). The early DVS shall be installed, on a temporary basis, at the SMC within 4 months of contract award. The early QAS may be delivered to the same site at the same time but, in any event, shall be delivered no later than two months after the early DVS.

Ideally, these early deliverables, supported by User Interface workstations and printers, shall support TDMS database building, display building, RTU/FRTU point-to-point communications protocol testing, OMS and EGAT SCADA/EMS data exchange testing using ICCP (secure ICCP if supported by the OMS and EGAT systems), and report generation testing prior to delivery of all other TDMS environments including all remaining elements of the PPE. Also refer to Clause 3.1.3.

The Contractor shall be responsible for developing all TDMS databases, displays, and reports including those created, checked, and used on the early DVS and QAS systems but shall be assisted in this activity by Authority personnel within the context of the PPE and PDE training that the Contractor is required to provide.

The early DVS shall include 2 workstations allowing 2 users to develop databases and/or displays at the same time. Databases and displays developed on the early DVS shall include those that are:

1) Basic to the Contractor's TDMS

2) Customized to meet Authority specific requirements and preferences

3) Web-based in support of Corporate users of the TDMS

4) Based on conversion and/or modification of displays and databases used by the existing DDC1 and DDC2 systems

5) Based on the import of Authority AutoCAD as well as GIS files containing power system and land-based data sent, for example, via a Contractor-provided connection to the Corporate WAN.

The early QAS shall also include 2 workstaions allowing 2 users to work on various PPE testing activities. In this respect, as a minimum, the QAS shall include:

1) Software and support tools for developing Authority required reports such as those that will be generated from data ultimately available from the Information Storage and Retrieval (IS&R) function

2) The capability to test and debug interface issues with existing FDIs using a listening mode.

3) The capability to verify the databases that will support TDMS interfaces with other computer systems such as the Authority GIS and MDMS and the EGAT SCADA/EMS

4) The capability to support any necessary incremental software additions and/or updates so that, on re-location at one of the data centers, for example, it may be used to support verification of the data acquisition and processing functions of the TDMS using actual data source connections prior to full point-to-point testing during the TDMS Site Acceptance Test (SAT).

5) The capability to be used by the Contractor to pre-commission the ported database.

Ultimately, both the DVS and QAS systems shall be upgraded and transformed into their full-functioned forms and integrated on-site as components of one of the TDMS main platforms to be installed at one of the Authority's two data centers.

14. Configuration, Redundancy, and Failure Management

The ability of the TDMS to perform its specified tasks under normal conditions and under conditions of hardware and software failure is of paramount importance to the Authority. This clause presents requirements for managing and monitoring TDMS hardware and software resources. In this respect, the TDMS shall be supported by the centralized management functions of the SME described in Clause 3.1.5.

14.1 Resource Groups and Interconnections

System resources shall be grouped in such a way as to meet system redundancy and/or performance requirements. In this respect, a group consisting of two or more similar resources (e.g., a group of

servers) may perform a subset of TDMS functions or tasks in a primary/backup manner, where the backup resource is only active in the event the normally active resource, i.e., the primary resource, has failed or been taken off-line. Alternatively, in a distributed manner, where the functions or tasks performed by the group are shared among the group's multiple resources, all of which are normally active. A resource within a group may also consist of a group of resources, e.g., a group of virtualized servers each of them hosting a group of virtual machines.

Interconnections, including those involving local and wide area networks, shall be provided among all resources within a group of resources, among all groups, and among all groups and all workstations. The state of each group or its individual resource connection to a network and the network itself shall be changeable by the user.

14.2 Operating State

The operating state of TDMS resources such as servers, processors, and peripheral devices[3] shall be monitored continuously to determine the system's condition when restart and failover operations take place. The definition of states will depend on the Contractor's TDMS design. For example, in the case of virtualized servers, the state of the virtual machines that they host shall also be monitored.

Within this context, the following states or their equivalent shall be supported:

1) *Normal* – The resource is operating per its normally assigned role, e.g., as a primary resource or as a backup resource in hot standby mode, or as an active resource among a shared group of replicated resources all of which are operating in their group's normal state and ready to serve as a shared backup facility should one or more of them fail.

2) *Abnormal* – The resource is operational but not in its normally assigned role, or in conditions that are not normal, e.g., a backup resource is now the primary resource due to primary resource failure, or a shared resource is operational in a situation where one or more of the resources in its group have failed. Such abnormal states may result from a user command.

3) *Failed* – The resource is non-operational, e.g., it is not communicating with other elements of the TDMS and is not capable of participating in any TDMS activity.

14.3 Database Backup

Database backup shall be supported so that TDMS operation may continue without issue in the event of a hardware or software failure. The backup database shall always be kept synchronized with the primary database. Failure of a resource shall not preclude access to current data by the resource or resources assuming the function of the failed resource. The backup database shall be protected from corruption due to such failures. The backup database as well as primary database shall be preserved during system input power disruptions of any duration.

[3] *This includes network devices, such as routers, switches, and firewalls, as peripheral devices. (Network interfaces may be considered as peripheral devices or as part of a processor or other device.)*

Changes to the quantity of information to be backed up because of adding or deleting database items shall be automatically accommodated by the backup function. The addition, deletion, or restructuring of the TDMS database shall be accommodated by the backup function without requiring changes to any software code.

14.4 Error Detection and Failure Determination

All resources shall be monitored for fatal and recoverable errors. All detected errors, including those leading to failures, shall be recorded for maintenance purposes. These records shall include the dates and times of the errors, reasons for the errors, and details concerning any resulting failures and subsequent automatic or manual return to service.

14.4.1 Hardware Errors

All fatal and recoverable errors of all hardware resources shall be detected. Each type of recoverable error shall be assigned a threshold. When the count of recoverable errors exceeds this threshold, a fatal error shall be declared, and steps taken to initiate whatever failover procedure may apply. Where multiple hardware resources share a common communications channel, the quantity of failed resources that constitute failure of the communications channel shall be individually specified for each channel.

14.4.2 Software Errors

Execution errors in functions that are not resolved by program logic internal to the function shall be considered fatal software errors. Examples of errors that may be resolved by internal program logic include failure of a function to achieve a solution due to violation of an iteration limit or arithmetic errors (such as division by zero). These errors shall produce an alarm informing the user of the error, but they shall not be considered fatal software errors.

Fatal software errors shall result in either termination of the function or shall be handled as a fatal resource (e.g., server/processor) error. The action to be performed shall be defined for each function. If the function is to be terminated, future executions of the function shall also be inhibited until the function is again initiated.

14.4.3 Reasonability of Data

All input data and parameters, whether collected automatically or entered by a user, shall be checked for reasonability and rejected as errors if they are unreasonable. All intermediate and final results shall be checked to prevent unreasonable data from being propagated or displayed to the user.

When unreasonable input data or results are detected, diagnostic messages clearly describing the problem shall be generated. All programs and the TDMS shall continue to operate in the presence of unreasonable data. All calculations using the unreasonable data shall be temporarily suspended or shall continue to use the last reasonable data.

14.5 Server/Function Redundancy and Failover

When failure of a resource, such as a physical or virtualized server or any function, in a redundant group of resources is detected, the TDMS shall invoke appropriate failover procedures so that functions or tasks assigned to the failed resource are preserved without disruption. The failed resource shall be marked as “failed” (or equivalent, such as “down”). The state of all resources used to preserve the functions of the failed resource shall be changed from “normal” to “abnormal”, or equivalent.

If a resource of the TDMS is damaged or performance degraded due to a cyber security incident, the affected resource shall be rapidly isolated from the rest of the TDMS, and the resource function or task subsequently restored in a timely manner.

Failover due to failure of a single resource, and subsequent restoration and restarting of the failed resource (or any replacement), shall not interrupt on-going system utilization.

14.5.1 Function Restart

Function restart, i.e., function assignment to servers and subsequent initiation, 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.

The restart logic shall determine the desired state of the assigned resources and the function or functions to be initiated. It shall also preclude conflicts among resources and functions, such as assigning too few or too many resources and erroneous duplication of functions in multiple resources. Immediately after initialization, the functions to be restarted shall be scheduled for execution.

14.5.2 Server Restart

Upon detection of a server failure, all servers providing for redundancy (and associated peripheral devices and interconnections) shall be reconfigured as necessary to support the server function or functions to be restarted. If servers are not available or prove insufficient to support function restart, the TDMS shall attempt to restart the failed server, which may require restart by user command only.

Server start-up shall be performed such that the operating environment of the server is established prior to restarting its functions. Establishment of the operating environment may include execution of self-diagnostics, reloading the operating system, and connection to and verification of communications with all appropriate networks. After server start-up, a function restart shall bring all relevant servers and functions to their appropriate state.

14.6 Device Redundancy and Failover

Devices shall be configured as redundant or non-redundant. When failure of a redundant device is declared, the TDMS shall invoke the appropriate device failover procedures so that on-line functions using the failed device are preserved. Server or function failover shall not be necessary to recover from device failure. On-line functions using a failed non-redundant device may be lost until the failed device is restored to service.

14.6.1 Device Failover

Device failover shall invoke an orderly transfer of operation to a backup device in the event of any primary redundant device failure. Multiple levels of failover shall be supported, i.e., if a primary device fails and its backup device then fails or if the backup device is failed at the time of failure of the primary device, the system shall attempt to use the backup assigned to the backup device. All functions associated with both failed devices shall then be directed to use the new device.

Device failover shall accommodate the following special cases:

1) *Printers* – Instead of an automated failover process, the user shall be able to direct output to any printer. However, the print services shall preclude the loss of information due to printer failures. This shall include information transferred to a printer, but not yet printed at the time of printer failure.

2) *Workstations* – Although workstations are configured as non-redundant devices, the failover logic shall ensure that all areas of responsibility assigned to the user of the failed workstation can be assigned to other workstations. If one or more areas are not assigned, the areas shall be assigned to a default user, and an alarm shall be generated.

3) *Backup and Archive Storage* – Long-term backup and archive storage devices need not be configured to support an automated failover process. Instead, the user shall be able to direct output to or read data from one out of two (or more) such devices. On the other hand, short-term backup and archive storage facilities shall provide a measure of automated failover. In this case, whereas their servers need not be redundant, their multiple solid-state drives shall provide drive backup capabilities via their distributed fault tolerant characteristics. This includes the capability to replace a failed drive by a spare “hot” drive.

4) *Networks and Network Devices* – Recovery from failures of networks and network devices shall be managed by the re-routing of communications. For example, failover to backup resources to recover from network failures shall be attempted only where no network route to the primary resource is available.

5) *Field Device Interface Communications* – Failover in these situations shall be on an FEP circuit or channel termination basis, i.e., if a single termination failure should occur on a redundant FEP, it shall not be necessary for all terminations to failover to the backup FEP.

6) *External System/GPRS Communications* - Failover in these situations shall be on a CNP circuit or channel termination basis, i.e., if a single termination failure should occur on a redundant CNP, it shall not be necessary for all terminations to failover to the backup CNP.

7) *Time and Frequency Support* – Failure of the Contractor’s internal time and frequency facility, receiving signals from the Authority’s Time and Frequency Facility, shall be managed as a device failure. If any component of the redundant internal facility is down, the TDMS shall report this as an alarm.

14.6.2 Device and Communications Reinstatement

Except for communications with data sources and other computer systems connected to the TDMS via the Corporate or TDMS network, failed devices shall be reinstated by user command only. Otherwise, failed communications to data sources or computer systems shall be periodically retried. When reliable communications are re-established, the data source and communications shall be automatically returned to normal operation with the TDMS.

Data sources may require the download of configuration information as part of the reinstatement process. Such configuration information may include report-by-exception dead bands.

14.7 System Restart

The TDMS shall automatically restart itself when input power is interrupted and restored. System restart shall include server and function start-up, initialization of all network devices, initialization of all peripheral devices, initialization of all communications with external data sources and computer systems, resumption of TDMS operation, and notification to the users that start-up has completed.

14.8 System Availability

14.8.1 General Requirements

Each TDMS function shall be classified as either critical or non-critical.

Every critical function shall be supported by sufficient redundancy to ensure that any single failure will only briefly interrupt the availability of that function. In this respect, critical functions associated with each data center shall be supported by at least two (2) independent resources, with all necessary input/output facilities, providing for redundancy. Failure to complete a critical function within a predefined time interval shall result in automatic transfer of its execution to an alternative resource if available. This shall include the capability to utilize backup resources at the other data center.

Non-critical functions need no redundancy in each TDMS data center because they may be terminated until restarted manually or may be executed at low priority until any necessary equipment repairs have been completed. On the other hand, depending on Contractor-provided backup features between data centers, the failure of resources used for non-critical functions at one data center may result in a manual and/or automatic restart of these functions on corresponding resources at the other data center.

The operation of all critical and non-critical functions shall be monitored, and all detected failures of these functions shall be separately logged (itself a critical function) for availability measurement and maintenance support purposes. These log entries shall include the dates and times of the failures and of the subsequent automatic or manual return to service.

Each automatic transfer to backup resources of one or more critical functions interrupted by a failure shall be completed with no loss of data. As a minimum, data coherency shall be maintained by performing integrity checks before committing and allowing for transaction rollbacks if needed. Functions that were scheduled to execute during the time that a transfer is occurring shall automatically execute following completion of the transfer.

For the system to be available, user TDMS interfaces via workstations must be stable. Restarts of other system components to clear workstation faults must be absolutely minimized.

14.8.2 Availability Requirements

The Contractor's proposal shall have described all failover features of the proposed TDMS design. This shall include the availability features associated with both critical and non-critical functions. Also refer to Clause 2 and 14.8.1.

On an individual data center basis, i.e., failover/backup capabilities between data centers notwithstanding, each TDMS platform shall be designed so that the total accumulative downtime of all critical functions, if executed on this platform only, does not exceed four (4) hours and twenty-three (23) minutes in any one (1) year period, resulting in an availability of 99.95%. As evidence of how the proposed TDMS at each data center meets this requirement, the Contractor's proposal shall have included detailed availability calculations.

Moreover, the Authority's availability requirement for the TDMS in its normal mode of operation shall be met, i.e., where the TDMS platforms at both data centers are serving as a common resource. Thus, the total accumulative downtime of all critical functions, as executed on the TDMS at either data center or possibly, depending on the TDMS design, at both data centers, shall not exceed fifty-three (53) minutes, representing an availability of 99.99%, in any one (1) year period or proportionally during the required Availability Test (refer to Clause 22.11). In addition to running the Availability Test to verify that the TDMS as actually delivered and handed-over to the Authority meets this requirement, the Contractor's proposal shall have included corresponding availability calculations.

Within this context, the TDMS shall be considered available when all functions identified in Clause 14.8.2.1 are operating as specified in accordance with their scheduled periodicities and required execution times, while all associated hardware specified in Clause 14.8.2.2 is also available.

The TDMS shall have no single point of failure, i.e., there shall be no hardware or software element that, because of its failure, renders the TDMS unavailable. This requirement shall specifically include all Contractor-supplied hardware, including power supplies, as installed and interconnected in data center enclosures provided by the Authority.

On an individual basis, all TDMS resources such as servers and devices on the TDMS network shall exhibit an availability of no less than 98%, where availability is calculated as: *(1- ratio of down time to required operational period) multiplied by 100*. The ability of TDMS individual resources to meet this requirement shall be verified during SAT.

14.8.2.1 Functional Availability

With respect to functional availability, TDMS functions normally sharing resources in such a way that they can execute on servers replicated within and/or across the two data centers, so that they are not affected by any single failure, are explicitly defined as critical. As a minimum, these functions include:

1) Failover and system restart functions without loss of data.

2) System configuration control.

3) Processing of acquired telemetered data (including calculations, database updates, limit processing, alarming, refreshing of displays, etc.).

4) All SCADA functions including data acquisition and supervisory control via field device interfaces.

5) Data exchange with the EGAT EMS and the Authority's GIS, OMS, AMS, and MDMS (independently of such external systems being redundant).

6) Information Storage and Retrieval.

7) Data storage functions supporting critical functions.

8) All HV/MV network applications in their real-time, study, and simulation modes.

9) User Interface functions supporting critical functions.

10) On-line diagnostics.

14.8.2.2 Hardware Availability

The TDMS hardware shall be considered available when sufficient resources and interfaces to data sources, remote workstations, and computer systems external to the TDMS are operating and the TDMS is satisfying its performance requirements. The term sufficient, as used in this paragraph, shall be interpreted as requiring the following minimum hardware complement to be operating:

1) At least one fully operational server (whether physical or virtualized) corresponding to each TDMS group of redundant/replicated servers.

2) Auxiliary SSD (NVMe preferred) memory sufficient to support the operating servers. In case of RAID memory units, no more than one SSD in each enclosure (chassis) shall be down.

3) At least one archive device.

4) At least one internal time and frequency facility.

5) Sufficient FEPs, channel interfaces, and other devices such that TDMS communications with all field device interfaces and other systems are supported.

6) Connections to the TDMS network sufficient to support communications with all nodes on the network including the external nodes on the Corporate WAN.

7) At least 50% of the remote workstations at each control center.

8) At least one multifunction printer at each control center.

15. Capacity and Performance

The TDMS shall be designed to meet the capacity and performance requirements defined in this clause. These requirements are based on estimated data sizing, data exchange periodicities, and functional performance characteristics for bench marking and do not necessarily match with the characteristics that will be experienced during actual operation of the TDMS. To ensure full understanding, the Contractor and Authority shall have worked together to review and agree on the final list of capacity requirements prior to contract signing.

The hardware and software configuration of the TDMS shall not impose restrictions that prevent the system from growing in capacity and performance to meet future Authority needs on a continuous and expanding basis, i.e., as new functions and data communications are added and the delivered capabilities of the TDMS become limiting, the Contractor's TDMS design shall enable the convenient addition of servers, processors, new or enhanced functionality, main and auxiliary memory, peripherals, and communications interface equipment.

Authority personnel shall be able to make all database and system changes to support the anticipated system growth through interactive procedures supplied with the TDMS and without assistance of the Contractor. No change in program code shall be necessary to implement such expansion. The Contractor shall provide all related documentation and shall demonstrate the expansion capabilities and features as specified to the Authority's full satisfaction.

All TDMS capacity and performance requirements shall be verified (tested) with all supplied security features enabled, such features as virus scanning, malware detection, system file integrity checking, firewall rule sets, intrusion detection, intrusion prevention, and security incident logging and reporting. An estimate of the overhead associated with the execution of the security features shall be calculated for review during system testing.

15.1 General Expansion Characteristics

TDMS expansion requirements are based on the most probable growth rates, the potential for new applications, and the desire to balance delivered TDMS costs against capabilities and, within this context, extend the life of the delivered TDMS with minimal disruption to system operations. Thus, the following expansion characteristics shall apply:

1) *Servers/Processors* - A growth path shall be provided with the delivered TDMS that allows the upgrading of computational power and main memory by means of field expansion and/or replacement of servers (or any processor unit). Such upgrades shall be possible by simply "changing out" the server and/or adding server processing capacity while retaining software and hardware compatibility. To the extent possible, upgrades based on installing additional components (such as CPUs) or replacing such components with their latest versions shall be taken into consideration.

2) *Computer Peripheral Equipment* - All peripheral equipment shall be standard products with standard interfaces capable of being replaced with more powerful and/or newer models without requiring additional hardware or software changes.

3) *Communications Equipment* - All data communications equipment shall be selected and integrated in such a way that the Authority may take advantage of new and improved data communications equipment as it becomes available. Standard equipment and standard protocols shall be used, and no modifications to standard hardware or software shall be allowed.

4) *User Interface* - The design of the user interface shall be such that the Authority may take advantage of new and improved user interface technology as it becomes available. Standard interfaces and equipment shall be used, and no modifications to standard hardware or software shall be allowed.

5) *Data Link Communications* - All data links shall conform to data communication standards. All communications shall be supported by the software protocol access interfaces such that the physical connections and details of the link procedures are transparent to the application programs in keeping with the OSI reference model.

6) *Operating System Software* - Operating system software shall be based on widely-used operating systems as specified elsewhere in the Technical Specifications. Full compliance to the relevant standards are required. No application program shall use a proprietary operating feature if the equivalent feature is already defined in the standard. The Authority shall be able to upgrade to higher-level operating system revisions as they are made available by the computer manufacturers without making modifications to the hardware, application software, support software, or the operating system's executive services (except as provided for by the computer manufacturers).

7) *Applications Software* - All application programs shall be written in a high-level language such as C or C++. In developing application programs, the Authority shall be able to utilize structured techniques and all standard high-level languages supported by the computer manufacturer. Interface libraries shall be provided to allow access to database elements, display services, and operating system services.

8) *Documentation* - The software development tools and documentation supplied shall be sufficient to allow the Authority to maintain the TDMS and design and integrate new capabilities into the TDMS without requiring additional design information. The use of proprietary designs for which design information will not be made available is absolutely prohibited.

15.2 Equipment Overview

The main equipment for each of the project's two data centers is identified in Exhibit 15-1, whereas the main equipment for each control center is identified in Exhibit 15-2.

The physical servers and their virtual servers/processors listed in Exhibit 15-1 are based on the provisional data center configuration depicted in Exhibit 3-1 and, as such, are subject to finalization based on the Contractor's proposed design that shall meet the TDMS capacity, performance, security,

and availability requirements. To this end, the Contractor's design shall include all necessary hardware and software even though it may not be expressly identified in these Technical Specifications.

Exhibit 15-1: List of Equipment for Each Data Center

Data Center Equipment	Quantity
PDE Physical Server (redundant)	**2**
• SCADA Server	1
• H/V Applications Server	1
• IS&R Server	1
• Database Server	1
PCE Physical Server (redundant)	**2**
• Front-End Processor	1
• ICCP Server	1
• Communications Network Processor	1
PPE Physical Server (non-redundant)	**1**
• Development Server	1
• QAS Server	1
DMZE Physical Server (non-redundant)	**1**
• High-Speed, High-Capacioty Data Historian	1
• WEB Server	1
SME Physical Server (non-redundant)	**1**
• Security Management Server	1
• Network Management Server	1
• Authentication Server	1
SIE Physical Server (non-redundant)	**1**
• SCADA Server	1
• HV/MV Applications Server	1
• Process Simulation Server	1
Network Equipment (as necessary)	
• Routers, Switches, Firewalls, etc.	1 lot*

*Final quantities per approved Contractor design details.

15.3 System Capacity

15.3.1 General

The Contractor shall supply sufficient TDMS data center and control center equipment to meet the Authority's capacity requirements.

The system capacity requirements include:

1) The function and database capacity requirements associated with Clause 15.3.2.

2) The processor and auxiliary memory capacity requirements associated with Clause 15.3.3 and 15.3.4.

3) The communications channel capacity requirements associated with Clause 0.

These capacity requirements shall be satisfied while meeting:

1) The performance requirements of Clause 15.4.

2) The availability requirements of Clause 14.8.

Exhibit 15-2: List of Equipment for Each Control Center

Control Center Equipment	Quantity			
	C1 & C2	Other 10 ADDCs	SMC	PDDC
Control Room				
• Remote Workstation (3-Monitor for TDMS access by Dispatcher/Supervisor)	7	5	5	2
• Workstation Furniture (console and chair)	7	5	5	2
• Dispatcher PC (for Corporate WAN access by Dispatcher/Supervisor)	7	5	5	2
• Multifunction Printer	1	1	1	1
• Black & White Laser Printer	2	2	2	1
• Video Display Wall (for 6 DDC1 control rooms only)	2	1 (C3, S1, N3)	1	-
• Interface for Existing Video Wall (DDC2 and SMC control centers only)	-	7 (DDC2 only)	1	-
Data Engineering Area				
• Remote Workstation (2-Monitor for TDMS access by Engineer)	5	5	10	-
• Workstation UPS (1 per workstation)	5	5	10	-
• Multifunction Printer	1	1	1	-
Network Test Sets				
• Notebook PC (with Protocol Analyzer and Network Sniffer S/W)	1	1	1	-
DAC Simulators				
• Notebook PCs (with SCADA S/W)	1	1	1	-
DTS Equipment				
• 3-Monitor Workstation (1 Trainer/6 Trainee workstations)	-	7 (C3 only)	-	-
Network Equipment				
• Routers, Switches, Firewalls, etc.	1 lot*	1 lot*	1 lot*	1 lot*

* Final quantities per approved Contractor design details.

15.3.2 Function and Database Capacity

As a minimum, the "delivered" capacity of the TDMS functions and its associated databases at each data center shall be dimensioned to accommodate:

1) HV/MV power system model sizing in accordance with the information listed in Exhibit 15-3, which represents the Authority's power system in all twelve service areas.

2) Data exchange with the various kinds of Field Device Interfaces (FDIs) deployed by the Authority. In this respect, total point quantities for each kind of existing FDI are presented in Exhibit 15-4.

3) Manually entered and calculated data in accordance with the sizing information presented in Exhibit 15-5. The source of the manually entered data accounts for all dispatchers at the 14 control centers, i.e., at the SMC, 12 ADDCs, and PDDC.

4) Data exchange with other systems such as the GIS, OMS, AMS, and MDMS. In this respect, sizing information related to the OMS and GIS is presented in Exhibit 15-6. AMS and MDMS sizing information will be determined during project implementation.

Exhibit 15-3: Power System Sizing Information

Power System Component	Quantity
HV Power Sources (e.g., EGAT generators or equivalent)	100
MV Power Sources (e.g., small power producers)	2,000
HV Substations	80
HV/MV Substations	500
Substation HV/MV Transformers	600
Substation Capacitor Banks	1,026
HV/MV Substation Circuit Breakers and Isolators	6,000
HV Buses	2,000
HV Line Circuit Switchers (Switch on Load and Remote Control)	200
HV Line Air-Break Switches	500
HV Line Segments	8,000
MV Feeders	5,500
MV Feeder Segments	2,000,000
MV Feeder Capacitor Banks (fixed)	4,000
MV Feeder Capacitor Banks (switched)	1,000
MV Feeder Line Reclosers	4,000
MV Feeder Line Recloser/Regulators	500
MV Feeder Remote Controlled Switches	15,000
MV Feeder Manual Switches	15,000
MV Feeder Dropout Fuse Cutouts	100,000
MV Feeder Distribution Transformers	500,000

5) Saved data as identified in Exhibit 15-7 for both the RDBMS and Historian databases associated with the required Information Storage and Retrieval (IS&R) functions.

6) Data supporting TDMS interoperation with the 14 control centers. Associated data sizing parameters are presented in Exhibit 15-8. This includes support for user access to the TDMS for purposes of on-line power system operations, and user access to the Historian and Web servers in the DMZ for off-line purposes.

At the time of system acceptance, the functions and databases shall be capable of accommodating at least a 100% increase in the delivered capacity without requiring regeneration, recompilation, or any other processing other than definition of the data by the Authority.

Exhibit 15-4: FDI Telemetered I/O Points

FDI Type	Protocol	Data Type	Quantity
SRTU, CSCS	Secure DNP 3.0	Status Analog Accumulator SOE Supervisory Control	380,000 200,000 1,000 200,000 120,000
FDCU (LRC, LRR, RCS)	Secure DNP 3.0	Status Analog SOE Supervisory Control	80,000 70,000 50,000 20,000
FRTU (Line Circuit Switches)	Secure DNP 3.0	Status Analog SOE Supervisory Control	2,000 1,200 800 400
FRTU (SCB)	-	Status Supervisory Control	10,000 2,000

Exhibit 15-5: Manually Entered and Calculated Data

Data Source	Data Type	Quantity
Manually entered	Status Analog Accumulator	15,000 10,000 1,000
Calculated	Status Analog Accumulator	10,400 50,000 1,000

15.3.3 Server Memory

At least 50% of the main memory of each TDMS physical server or processing unit shall be unused (spare) and immediately available for the sole use of the Authority at the time of system commissioning. This shall also apply to the memory allocated to each server's virtual machine. In addition, at the time of system commissioning, the main memory shall be expandable to two (2) times the installed memory capacity.

15.3.4 Auxiliary Memory

At least 50% of the auxiliary memory of each TDMS processing unit shall be unused (spare) and immediately available for the sole use of the Authority at the time of system commissioning. In addition, each auxiliary memory unit shall be expandable up to two (2) times its capacity. These requirements shall also apply to memory dedicated to backup and archiving data storage facilities including IS&R data storage.

Exhibit 15-6: Data Exchange with Other Systems

Other System	Protocol	Data Type	Quantity
GIS	FTP/SFTP/CIM	Data File (1 GB per ADDC)	1
OMS	Secure TASE.2	Status Analog Event	100,000 200,000 100,000
	SFTP	Data File (MB)	50

Exhibit 15-7: IS&R Data

Function/Data	Quantity	Periodicity	Retention Period	Working Area
Alarms and Events	60,000/day	On Occurrence	2 Months	1 Month
Sequence of Events	48,000/day	On Occurrence	2 Months	1 Month
Analogs (30-min. peak, minimum, and average values)	All analogs	30 Minutes	24 Months	1 Month
State Estimation (SE) Save Cases	1	30 Minutes	6 Months	1 Month
Power Flow (PF) Save Cases	120	Daily	12 Months	1 Month
Feeder Power Losses	All feeders	30 Minutes	12 Months	1 Month
Real Power, Reactive Power, and Current Values At Time of Breaker waker and Before s	2,000/day	On Occurrence	12 Months	1 Month
Continuous Data Recording	• All analogs • Status of all power system equipment (CB, DS, RCS, etc.)	Upon change Upon change	24 Months 12 Months	3 Months 1 Month

Exhibit 15-8: TDMS/Control Center Interoperation Parameters

Parameter	Quantity
Minimum Number of Remote Workstations	
• Dispatcher/Supervisor (3-monitors)	71
• Data Engineering (2-monitors)	70
• DTS Trainer/Trainee (3-monitors)	7

Parameter	Quantity
Minimum Number of Concurrent TDMS Remote Users	
• Control room users	71
• Data engineering room users	100
• DTS users	7
• External users connected via the Corporate WAN	500
Number of AORs	360
Number of User Roles	12
User Interface per Workstation	
• Number of user-defined windows per monitor	4
• Trend curves per display	5
• Maximum number of trend displays at one time	4
• Number of alarm classes	8
• Alarms presented on the alarm summary	2,000
• Events presented on the event summary	5,000
Line Limits	
• Operating Limits (3 pairs x 12 service areas)	36
Tags	
• Number of Tag Types	16
• Number of Tags per Point	8
Switching Management System	
• Number of saved switching orders	1,200
Load Shedding and Restoration	
• Number of Load Blocks	1,000
• Number of Points per Block	15
IS&R	
• Simultaneous users	400
• Development users	30
IS&R (DMZE)	
• Simultaneous users	200
• Development users	30
Web Server	
• Simultaneous users	200
• Development users	30
HV/MV Power System Applications	
• Simultaneous users (real-time and study)	100
• Simultaneous users (simulation)	50
• Save cases	400
Load Forecast Function	
• Simultaneous users	50
• Day Types	15
• Length of Study (days)	7
• Time Interval (minutes)	15
• Save cases	150
Equipment Outage Scheduling	
• Months in the future	3

15.3.5 Communications Channel Capacity

As a minimum, each TDMS master station shall be equipped to accommodate all communications channels that are required to interconnect the TDMS to the quantity of Field Device Interfaces (FDIs) that will exist at the time of TDMS commissioning. These are the FDIs that relate to the Authority's SRTU, CSCS, RCS, LRC, LRR, and SCB devices. In addition to existing FDIs, they will include the

new FDIs (also referred to as FDCUs) that will be installed as part of DDIP, i.e., under contracts separate from the TDMS contract. On this basis, considering their association with different types of device deployed by the Authority, the expected quantities of FDIs at the time of TDMS commissioning are identified in Exhibit 15-9.

In addition to accommodating all FDIs that will exist at TDMS commissioning, each TDMS shall also be equipped with a 100% spare communications channel capacity to allow for even more FDIs to be accommodated, i.e., the future FDIs that the Authority will deploy after commissioning and acceptance of the TDMS.

Exhibit 15-9: FDI Quantities at Time of TDMS Commissioning

Service Area	SRTU/CSCS	RCS		LRC	LRR	SCB
		Existing FDI	New FDI			
C1	71	526	805	95	2	45
C2	82	606	793	28	1	26
C3	53	428	789	136	9	23
N1	42	391	225	122	10	85
N2	30	450	189	154	9	92
N3	30	266	209	158	11	14
NE1	41	403	208	123	8	86
NE2	29	413	225	209	19	95
NE3	33	397	280	83	29	71
S1	21	253	300	118	2	25
S2	23	364	324	126	2	25
S3	29	370	223	110	0	66
Total	**484**	**4867**	**4570**	**1462**	**102**	**653**

15.4 System Performance

Satisfaction of the system performance requirements shall be verified during factory and site tests as specified in Clause 22.9 and Clause 22.10 of these Technical Specifications. It is the Authority's intent that the TDMS exhibits consistent performance even when operating in a degraded configuration. To this end, the TDMS shall satisfy the performance and capacity requirements of these specifications under the following configurations:

1) The "normal" configuration with all system components operating.

2) A degraded configuration where one processor of each redundant server group is assigned to the "failed" state.

As in the case of system capacity, it is the TDMS equipment operating at only one data center and supporting all interfaces that must meet the performance requirements as presented in the following sub-clauses. These interfaces, for example, are those with other systems, the Authority's 14 control centers, and all FDIs throughout the Authority's entire service territory. The performance requirements shall apply to the TDMS applications whether used in their normal real-time and study modes or in their simulation mode, e.g., the simulation mode that supports the Dispatcher Training Simulator (DTS) facility (refer to Clause 20.23).

15.4.1 System Activity Scenarios

TDMS performance shall be tested under the following scenarios:

1) The base scenario (Clause 15.4.1.1) on top of which the steady-state and high-activity scenarios are layered.

2) The steady-state scenario (Clause 15.4.1.2) representing field operating conditions during a typical 60-minute period.

3) The high-activity scenario (Clause 15.4.1.3) representing field operating conditions during a 20-minute period such as might be experienced during a major power system disturbance.

15.4.1.1 Base Scenario

The following base scenario shall apply to both the steady-state and high-activity scenarios:

1) Except for testing under abnormal degraded conditions, the TDMS shall be configured with all hardware and all functions operational. Per Clause 0 the TDMS shall be equipped to not only accommodate the intended quantity of FDIs at system commissioning, but also the required spare capacity of 100%.

2) For the TDMS under test, its resources at its data center shall perform all data processing required to support synchronization with the replicated resources at the other data center as well as interoperation with the 14 control centers, the Historian and Web Servers, the Authority's GIS, AMS, and OMS, and the EGAT SCADA/EMS. As necessary, such interoperation shall be simulated.

3) The execution parameters of all system functions shall be determined by the Authority.

4) System functions at all control centers shall execute at the periodicities and execution times specified in Exhibit 15-10.

5) Software and databases shall be configured in accordance with the requirements of Clause 15.2.

6) Contents of the databases and display and report definitions shall be determined by the Authority but will not be greater than the delivered capacity specified in Clause 15.2.

7) The hour change shall occur so that all data acquisition and processing associated with hourly system functions, including report generation, are executed.

Exhibit 15-10: Function Periodicity and Execution Time

Function	Periodicity	Maximum Execution Time		Notes
		Steady State	High Activity	
Data Acquisition (any data source including other computer systems)	2 second status 10 second analog	1 second	1 second	Time from receipt of message with changed data until processing complete, change stored in database, and alarm list updated.
Network Topology/ Coloring	As required by power system conditions	1 second	1 second	Time from single event until stable network/color is reached.
Supervisory Control (exclusive of communications)	As required by Dispatcher or application	1 second	1 second	Time from execution of command until command exchange with data source.
Time & Frequency Update	1 second	-	-	-
Distribution Load Forecast	30 minutes (update mode)	5 seconds	8 seconds	Using 15-day study.
Fault Level Analysis	On demand	2 seconds	3 seconds	MV network solution per single feeder fault.
HV and MV State Estimation	On demand, on status change, and every 15 minutes	3 seconds	4 seconds	From request until presentation of HV and MV network solutions.
HV and MV Distribution Power Flow	On demand	2 seconds	3 seconds	From request until presentation of HV and MV network solutions.
Volt/Var Control as applied to HV and MV networks	On demand and every 15 minutes	5 seconds	8 seconds	From request until presentation of HV and MV network solutions.
Fault Location, Isolation, & System Restoration	As required by power system conditions	60 seconds	90 seconds	Time from permanent single feeder fault detected by DMS until a restoration recommendation is presented.
Data Engineering (Network model incremental update)	On demand	5 Minutes	8 Minutes	Time from initiating incremental update in DS to update in PDE.

8) Each monitor at all workstations shall present all “common information” deemed by the Authority to be part of the normal display arrangement. Such common information may include:

a) Display title and window border.

b) Alarm zone.

c) Dispatcher message area.

d) Time and date area.

e) Top-level menu bar.

9) Each dispatcher workstation shall have four updating windows open to show:

a) The global alarm list.

b) A distribution system overview display in one of the windows and, for 10% of the time, panning and zooming of this display shall be performed.

c) Two displays selected by the Authority for performance testing, including any application input or output display or trending display.

10) Each data engineering workstation shall have two windows open, showing a distribution overview display and any other display selected by the Authority.

11) Each video wall display (as may be simulated) shall show the current power system status and alarms as well as an overview of the power system.

15.4.1.2 Steady-State Scenario

The steady-state scenario shall consist of the base scenario and the following additional activities over a sixty-minute period:

1) Twenty-five percent (25%) of all analog points shall change sufficiently that they are acquired and processed by the TDMS.

2) Thirty (30) alarms per minute (fifteen status alarms and fifteen analog alarms) shall be generated for each control center's area of responsibility and processed. Each of these alarms may be acknowledged within sixty (60) seconds at the Authority's discretion.

3) One new display shall be called into one of the windows at each workstation every sixty (60) seconds.

4) Two (2) data entries shall be executed at each workstation every sixty (60) seconds.

5) One supervisory control sequence consisting of the opening and closing of one field device switch shall be executed at each dispatcher workstation every ten (10) minutes.

6) The Switching Management System application shall be executed from each control center to create at least two (2) different switching orders, each consisting of at least five (5) open and five (5) close switch commands. One of these switching orders shall also be implemented during the steady-state scenario's test period.

7) One five per cent (5%) rotating load shed and restore sequence shall take place in areas of responsibility associated with three (3) control centers over a 30-minute period.

8) The State Estimation function shall execute periodically every minute to present the on-line state of the entire HV/MV power system network.

9) The HV network Contingency Analysis function shall execute following each SE execution.

10) All other EMS and DMS functions shall be executed on-demand under Authority defined conditions from each control center at least four (4) times during the test period. For the FLISR function, this shall include a simulated feeder fault between remote controlled switches that shall require automatic fault location, isolation, and subsequent power restoration to all healthy feeder segments. After a defined interval of time, it shall also include automatic switching to return the feeder to its pre-fault configuration.

11) One dispatcher workstation at two (2) control centers shall be used in simulation mode for a period of thirty (30) minutes during which time an Authority defined scenario shall take place along with at least one execution of FLISR and the HV/MV Power Flow and Volt/Var Control functions. In addition, the SE application and CA functions shall execute automatically in sequence every minute.

12) Five (5) ad hoc queries of IS&R data and five report requests of IS&R data from one dispatcher workstation at all control centers shall be made during the scenario. Each query or report shall, on average, include 500 items.

13) An incremental import from the GIS (as may be simulated) shall be accomplished followed by an update to the on-line TDMS.

14) Two (2) typical data exchanges with the EGAT EMS and the Authority's OMS, AMS, and MDMS (as may be simulated) shall take place.

15) At least ten (10) dispatcher PCs shall be used at least twice to access information made available by the TDMS at the Web Server.

16) In parallel with the continuous recording process of the Historian IS&R, five (5) dispatcher PCs shall be used to access, view, and use the recorded data to complete a typical report.

15.4.1.3 High-Activity Scenario

The high-activity scenario shall consist of the base scenario and the following additional activities over a twenty-minute period:

1) Fifty percent (50%) of all analog points shall change sufficiently that they are acquired and processed by the TDMS.

2) A burst of at least 12,000 alarms within the first sixty (60) seconds, i.e., 500 status alarms and 500 analog alarms per ADDC, shall be generated and processed within the first sixty seconds of the scenario. Fifty (50) alarms per minute, e.g., 25 status alarms and 25 analog alarms per control center, shall be generated and processed for the remainder of the scenario. Each of these alarms may be acknowledged within sixty (60) seconds at the Authority's discretion.

3) One new display shall be called into one of the windows at each workstation every thirty (30) seconds.

4) Five data entries shall be executed at each workstation every thirty (30) seconds.

5) One supervisory control sequence consisting of the opening and closing of one field device switch shall be executed at each dispatcher workstation every five (5) minutes.

6) The Switching Management System application shall be executed from each control center to create at least three (3) different switching orders, each consisting of at least five (5) open and five (5) close switch commands. One of these switching orders shall also be implemented during the high activity scenario's test period.

7) One 10% rotating load shed and restore sequence shall take place in areas of responsibility associated with four (4) control centers over the complete high activity test period.

8) The State Estimation function shall execute periodically every minute to present the on-line state of the entire HV/MV power system network.

9) The HV network Contingency Analysis function shall execute following each SE execution.

10) All other EMS and DMS functions shall be executed on-demand under Authority defined conditions from each control center at least three (3) times during the test period. For the FLISR function, this shall include a simulated feeder fault between remote controlled switches that shall require automatic fault location, isolation, and subsequent power restoration to all healthy feeder segments. After a defined interval of time, it shall also include automatic switching to return the feeder to its pre-fault configuration.

11) One dispatcher workstation at three (3) control centers shall be used in simulation mode for the entire test period during which time an Authority defined scenario shall take place along with at least one execution of FLISR and the HV/MV Power Flow and Volt/Var Control functions. In addition, the SE application and CA functions shall execute automatically in sequence every minute.

12) Ten (10) ad hoc queries of IS&R data and five (5) report requests of IS&R data from one dispatcher workstation at all control centers shall be made during the scenario. Each query or report shall, on average, include 500 items.

13) An incremental import from the GIS (as may be simulated) shall be accomplished followed by an update to the on-line TDMS.

14) Two (2) typical data exchanges with the EGAT EMS and the Authority's OMS, AMS, and MDMS (as may be simulated) shall take place.

15) At least ten (10) dispatcher PCs shall be used at least twice to access information made available by the TDMS at the Web Server.

16) In parallel with the continuous recording process of the Historian IS&R, five (5) dispatcher PCs shall be used to access, view, and use the recorded data to complete a typical report.

15.4.2 Resource Utilization

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. For example, server average utilization may be calculated as busy time divided by total time. Network average utilization may be calculated as the quantity of data transferred (Mbytes) divided by the network data rate (Mbytes/second) multiplied by total time (seconds).

The Contractor shall supply software to automatically determine resource utilization as described in Clause 0. The following utilization requirements are applicable to system performance under factory and site test conditions. The Contractor must demonstrate in the field that these utilization requirements have been met prior to acceptance of the TDMS.

15.4.2.1 Steady-State Utilization

Requirements related to the average utilization of each system resource during the steady-state scenario are listed as follows:

1) Utilization of the processing capacity of any resource used to execute application functions shall not exceed 35%.

2) Utilization of the transfer capacity of each auxiliary memory device shall not exceed 30%.

3) Utilization of any non-deterministic network (such as Ethernet) shall not exceed 5%; the loading of any deterministic network shall not exceed 10%.

15.4.2.2 High-Activity State Utilization

Requirements related to the average utilization of each system resource during the high-activity scenario are listed as follows:

1) Utilization of the processing capacity of any resource used to execute application functions shall not exceed 40%.

2) Utilization of the transfer capacity of each auxiliary memory device shall not exceed 40%.

3) Utilization of any non-deterministic network (e.g., Ethernet) shall not exceed 10%; if applicable, the loading of any deterministic network shall not exceed 25%.

15.4.3 User Interface Response

The TDMS shall provide rapid and consistent response to power system events and user inputs. System responsiveness to events and inputs during factory and site testing shall satisfy the following requirements that relate to the steady-state and high-activity scenarios.

15.4.3.1 Display Request

The display response time is defined as the elapsed time from a user's request for a display (initiated by a menu selection, function key activation, or cursor target selection) until the requested display is presented complete with current data retrieved from the system databases.

Display response times shall be demonstrated for the system operating in the steady-state and the high-activity scenarios. The display response time for each request shall conform to the display response time requirements shown in Exhibit 15-11.

The Authority may choose any or all system displays for this test.

15.4.3.2 Alarm and Event Annunciation

Any change of a data item that results in the generation of an alarm shall be reported by audible and visual indications within the times shown in Exhibit 15-11. The alarm response time shall be measured from the time any of the following actions occurs:

1) The system receives a message from a data source containing a changed data item that produces an alarm condition, where received means the last bit of the message passes across the interface with the system but is not yet processed.

2) A periodic system function calculates or otherwise generates a data item that it stores in the database and which produces an alarm condition.

3) The execution of a system function initiated by a user action or other request calculates or otherwise generates a data item that it stores in the database and which produces an alarm condition.

The measurement of the alarm response time will end at the time the alarm condition has been completely processed, recorded in the system database, and presented in all windows with displays that include the value in alarm or any presentation of the alarm condition.

15.4.3.3 User Requests

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. Completion of the request shall include production of all results, storage of the results in the system database, and updating of all relevant displays. User request response requirements for specific tasks are presented in Exhibit 15-11. The default response time presented in Exhibit 15-11 shall be met for all other user requests not specifically included in these Technical Specifications.

Exhibit 15-11: User Interface Response

Action	Scenario Maximum Response Time		Notes
	Steady State	High Activity	

Action	Scenario Maximum Response Time		Notes
Default response	1 second	1.5 seconds	98% of actions complete within max. time, 100% within 1.5 x max.
Schematic display request	1 second	2 seconds	98% of actions complete within max. time, 100% within 1.5 x max.
Geographic display request	2 seconds	3 seconds	98% of actions complete within max. time, 100% within 1.5 x max.
IS&R display request	1 seconds	1.5 seconds	98% of actions complete within max. time, 100% within 1.5 x max.
Display data update (following initial presentation of data)	1 second	1 second	4-second periodicity, 98% of actions complete within max. time, 100% within 1.5 x max.
Alarm and event annunciation (from time of system receipt)	1 second	1.5 seconds	98% of actions complete within max. time, 100% within 1.5 x max.
Viewport creation	1 second	1.5 seconds	98% of actions complete within max. time, 100% within 1.5 x max.
World-map panning	Continuous (5, 20-pixel steps per second)	Continuous (5, 20-pixel steps per second)	No visible flicker.
World-map zooming	Continuous (2, 10% steps per second)	Continuous (2, 10% steps per second)	No visible flicker.
Pop-up menu, pull down menu, dialog box, etc. (assumes no function processing required)	1 second	1 second	Not to exceed 150% of the maximum under any condition.
Display hardcopy	60 seconds	90 seconds	98% of actions complete within max. time, 100% within 1.5 x max.
Workstation user logon	10 seconds	10 seconds	98% of actions complete within max. time, 100% within 1.5 x max.

15.4.4 Resource Monitoring

Resource utilization shall be measured, calculated, and displayed for the TDMS servers, processors, devices, and networks. The minimum parameters to be presented include:

1) Time utilization (percent processor utilization) of each function per server.

2) Time utilization (percent SSD utilization) of each function per SSD.

3) SDD data transfers per SDD.

4) Performance of routers, switches, firewalls, and other SNMP-enabled network devices.

Statistical sampling and accumulation techniques shall be used to collect these parameters over a user-selected time interval. The user shall be able to specify the study period over which samples are

collected and the sampling frequency. Typical study periods shall be ten seconds to sixty minutes, and typical sampling frequencies shall be once per two milliseconds to once per fifty milliseconds.

15.4.5 Configuration Management

The required performance characteristics dependent on the Contractor's TDMS configuration management features are presented in Exhibit 15-12. These features concern how long it takes for the TDMS database to be backed up and how quickly function and device failovers, recoveries from communication failures, and system and processor startups can be completed.

Exhibit 15-12: Configuration Management Performance

Action	Performance
Backup database update	Within 60 seconds.
Detection and annunciation of processor or device failure and initiation of restart/failover process	Within 10 seconds.
Function restart/processor failover Restart/failover from backup database Restart/failover from empty or initialization database	 Within 30 seconds. Within 30 seconds.
Recovery from communications failure LAN or WAN failure Field device interface communications failure	 Within 30 seconds Within 30 seconds
Device failover	Within 10 seconds
Complete system startup (from power-off condition)	Complete, with all functions scheduled for execution, within 15 minutes
Processor startup	Complete, with all functions scheduled for execution, within 5 minutes

Exhibit 15-13: Software Maintenance

Action	Performance
Complete database regeneration from RDBMS	2 hours
Complete system software build, including operating system, applications, and databases	6 hours
Software build of all applications and databases	3 hours
Software build of single application and database	30 minutes
Installation of a single new display including distribution to all workstations	60 seconds
Reinstallation of all displays	60 minutes
Update of a database parameter and propagation of the change to the source data	60 seconds

15.4.6 Software Maintenance

The required TDMS performance characteristics that relate to database generations and builds, system software and application builds, display installations, and database parameter changes are presented in

Exhibit **15-13** above.

16. User Interface/Visualization

Users of the TDMS will interface with the TDMS at workstations. Interface functionality, however, shall be limited by the user's logon privileges. For example, users connected to the Corporate WAN and authorized to access the Web-server in the TDMS DMZ shall only be allowed to view TDMS displays and only those displays corresponding to the specifics of their authorization. This shall be possible by using their workstation's browser, e.g., Internet Explorer.

The user interface features of the TDMS shall include those that can be provided by video display walls and multifunction printers. In this respect, Authority existing as well as Contractor-provided video display walls shall be utilized. The existing video display walls to be utilized (along with their controllers) are those that were provided for the DDC2 project (i.e., one video wall display at each of 7 DDC2 control centers) and the video display wall more recently installed at the SMC control center. These video display walls are BARCO products, and all of them use the Linux operating system. Further details will be provided as needed during project implementation.

16.1 Visualization Design

The visualization functionality supplied with the TDMS shall employ the latest full-graphics technology with Situational Awareness tools. Displays shall be built only once, after which they shall be viewed and used for TDMS interaction from any workstation.

Situational Awareness tools shall have advanced features such as Drag and Drop, Advanced Alarming, 3D visualizations, world maps, contouring, use of widgets, meters, dials, and other objects. These features shall be used to enhance operations and significantly enhance situational awareness in the control room. There shall be no limitation in number of user-based desktops. These shall include but shall not be limited to fully customizable dashboards including data widgets that relay vital information to dispatchers and other users of the TDMS such as operations managers. Some of the Out-of-the-box objects and Widgets shall include Meters, Dials, Gauges, LEDs, Knobs, Buttons, and Pie, Bar, Line, and Plot Graphs.

16.2 User Interface Guidelines

16.2.1 User-System Interaction Guidelines

The user procedures for interacting with the TDMS shall be simple, fast, and unambiguous, and shall be "fail-safe" to guard against inadvertent user errors. In this respect, the following design guidelines shall be followed:

1) Single-step procedures (i.e., initiation of functions by clicking a pushbutton or a display symbol that is always shown in the appropriate application window) are required, whenever feasible, for frequently used functions and for critical functions.

2) Common and frequently employed actions shall be initiated from toolbars. One or more toolbars, specific to an application or function that is currently active, shall be shown in each window.

3) The use of pop-up dialog menus which overlay portions of one or more windows shall be kept to a minimum.

4) Multi-level menus shall be used only for the presentation of hierarchies of options and shall have the minimal number of levels needed.

16.2.2 Information Presentation Guidelines

The following design guidelines shall be followed for information presentation:

1) Power system information shall be organized and presented to the user in a manner that allows the user to be immediately aware of any condition requiring urgent attention, to quickly grasp the most significant aspects of a situation, and to have fast access to related data for further investigation.

2) Application programs shall not merely present the results of their calculations, but shall present in highlighted form, the most significant results.

3) Displays built by the Contractor shall be constructed with systematic use of borders or frames to visually group information that logically belongs together. For example, displays for training simulation may be shown in a color different than real time or may be distinguished by a water mark.

4) Headers shall be placed on displays and reports using larger fonts and/or bold characters.

5) Color shall be used to distinguish different dynamic states and to highlight important information but shall not be used for decorative purposes.

6) On-line help shall be readily available on displays and shall be designed to present useful information and explanations to the inexperienced user. The TDMS shall conform as much as possible to the Microsoft Windows standards for the on-line help function (e.g., pressing the F1 function key shall open the Help directory window).

7) Messages to users shall be easily understood. In this respect, cryptic messages shall be avoided.

8) When requesting input from the user, the TDMS to the maximum extent possible shall ensure that the user has on view all information needed to decide on the requested input.

9) Where possible, the system shall offer menu-selectable default entries for the most common or most likely data entries.

10) The TDMS shall not require the user to make repeated entries of the same data but shall provide a means for quickly copying data from one set of entry fields to another through copy/paste and drag/drop techniques.

11) When a data entry must be one of a defined set of possibilities (e.g., a file name or substation name), the possible entries shall be presented to the user in a scrollable list, and selection of the desired option shall be by clicking the desired entry. If a search engine is used, search shall be possible by keying in the first 2 or 3 characters.

12) A display shall be able to present any combination of telemetered and calculated data types (e.g., historical as well as analog and status values) and any combination of display types (e.g., schematic, graphical, and trend displays).

The detailed design of the user interface, including navigation trees and menu bars, the format and contents of dialog menus, the colors of display features such as menu bars, window borders, display background, and the operational procedures, shall be selectable in the database definition process. The initial design to be included in the TDMS shall be subject to Authority approval.

16.2.3 Look-and-Feel

The Contractor shall provide a full-graphic user interface for the TDMS workstations, whose functionality and behavior shall conform to the norms of Microsoft Windows applications. A design that takes full advantage of the features of the Windows graphical user interface capabilities is required. The appearance of the user interface and the methodology of user interaction with the TDMS and all applications shall follow the “look-and-feel” of the latest revisions of Microsoft Windows and the corresponding Windows Office applications.

A consistent approach is required for the formatting of displays, the graphic presentation of power system devices, the use of color and other display features for highlighting events and exceptions, and for every other aspect of display appearance. The appearance of power system devices (e.g., their shape, color, background color, and blink-related features) and the use, for example, of fonts and colors in display titles and other text shall be subject to approval.

16.3 Visualization Features

The following features shall be included in the TDMS user interface. Alternatives may be offered but must be functionally equivalent to the features specified.

16.3.1 Thai Alphabet

The user interface shall support displays and messages (such as event and alarm messages) that use Thai as well as English alphanumeric text. The ability to use the full Thai alphabet, including Thai numerals, shall be provided. It shall be possible to produce and display text that intersperses Thai and English characters. All workstation keyboards shall accommodate Thai as well as English characters.

Any font available in the operating system provided by the Contractor, whether applicable to Thai or English, shall be available for use in any kind of TDMS display. In addition to fixed size fonts, scalable fonts that change in size with zooming are required. The fonts to be used in displays shall be selectable.

Within this context, note that the TDMS shall not contain any text that is other than English or Thai. For example, if the baseline system used to develop the TDMS contains any text in a language other than English or Thai, it must be removed completely or, if necessary, replaced by the English or Thai equivalent. This applies to all elements of the TDMS such as databases, displays, and logs.

16.3.2 Common Features

The user interface shall include the following common features associated with workstations:

1) Time and date shall be presented on each workstation as always visible, but not necessarily on each display.

2) An alarm window shall be presented on each workstation.

3) An indication that audible annunciation of alarms has been suppressed.

4) 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.

5) Multiple navigation tools including alphanumeric display call-ups, main menus, pull down menus, etc.

6) A navigation aid pertaining to any display in a monitor's active window that is presented in world coordinate space. The navigation aid shall represent a condensed view display of the world coordinate space. Highlighting within the navigation aid display shall indicate the portion of the world coordinate space that is currently presented in the active window.

7) An area for the presentation of user guidance messages and an area for the presentation of user help information.

16.3.3 Windows Management

The combined monitors of a workstation shall be managed as a single monitor or "desktop". Thus, windows may be opened at any position within the desktop and moved continuously from monitor to monitor across the full desktop. As a minimum, user workstations shall support up to eight (8) windows on each monitor in addition to the dedicated window for information such as date and time.

There shall be only one active window at a workstation. The active window shall be identified by highlighting its title bar, and it shall be the focus and conduit for all user interactions such as display call-up, navigation through displays, program execution, and dialog interactions. An *implicit* rule for the active window shall be as follows: the window on which the cursor comes to rest shall become the active window without clicking when it is in the window.

In general, all windows shall have the same basic structure and include:

1) Window border.

2) Title bar.

3) Maximize, Minimize, Restore, and Close buttons.

4) Scroll bars, when the display spans beyond the window. The magnitude and position of the slider of the scroll bar shall represent the size of portion of the display that is currently being shown relative to the full size of the display and the position of the shown portion within the display.

5) Mode/Case identification, i.e., the operational mode (real-time, study, simulation, etc.) of the function running in the window shall be shown very distinctly.

6) A Toolbar from which pull down menus can be called.

7) Application area, i.e., the main area of the window from which the TDMS functions and applications are operated.

It shall be possible to drag a border of a window to increase or decrease its size in one direction, or to drag a corner to increase or decrease the window size in the two adjacent directions. It shall be possible to drag any window that does not fill the whole screen to any location, even when part of the window extends beyond the screen. Any one window shall not be permitted to shrink to the point where the window title cannot be read, and window titles shall be designed so that the currently loaded windows can be identified on the task bar (for example, “Alarm Summary” and not “Window 1”).

It shall be possible for every user of the TDMS to define and save the user’s individual screen layout for each monitor of the user workstation, i.e., the preferred number of windows on each monitor of the user workstation and their size, position, color, text, and content. When a user logs on to a user workstation, the user’s pre-defined dedicated screen layouts shall appear.

Fully documented window management capabilities shall be provided to allow window creation, deletion, movement, and re-sizing.

16.3.4 Display System Requirements

The user will operate from several major types of power system display, including but not limited to:

1) Schematic and geographical diagrams of the HV transmission lines, MV distribution lines, and related substations.

2) Tabular displays many of which will also include imbedded graphical data representations.

3) Queries-based displays.

All such displays shall be dynamic, i.e., the appearance of objects in these displays shall reflect the values and attributes in the real-time database, so that they can serve as effectively as possible as the main tool for monitoring and controlling the power system.

To support creation of these displays, the Contractor shall import and convert all relevant data that will be available from Authority GIS and existing DMS facilities. This shall include the ability to import and convert power system network model and associated land based data such as:

1) Element names including, for example, substations, buses, lines, transformers, circuit breakers, and loads.

2) All required attributes associated with these elements or objects such as impedance, line length, etc.

3) Normal status of switches including circuit breakers and disconnects.

4) Geographical information such as physical location of substations, feeder poles, feeder sections, power apparatus (including distribution transformers), field equipment, etc.

The presentation of such data on the TDMS displays shall be capable of being turned on and off manually as well as by zoom level, etc.

16.3.5 Display Selection

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

1) Selection from a menu display.

2) Cursor target operation on any menu, graphic, or tabular display.

3) Selection of an alarm on an alarm summary or the alarm window followed by a display request command.

4) Entry of a display name in a display select field.

5) Forward and reverse paging through a series of displays. Paging forward from the last page of a series shall present the series' first page. Paging backward from the first page of a series shall present the series' last page.

6) Operating a display recall cursor target in a window. This shall cause the display that was on view immediately prior to the current display to be recalled. The Authority prefers that the most recent displays called within the window be stored in a circular recall list and that successive recall actions recall progressively "older" displays.

The user shall be provided with window selection techniques to independently direct a display to any window at the workstation.

16.3.6 List Displays

Certain displays will present data in a text "list" format, i.e., a tabular format, consisting largely of rows of similar entries. Reports presenting time-sequenced data, alarm summary displays, and application program results are examples of list displays.

The TDMS shall support the following techniques for moving through the data presented on list displays:

1) Scrolling via slider bars.

2) Paging up and down.

3) Entry of a page number.

Paged displays (as opposed to scrolling displays) shall include a "page M of N" message on each page of the display. Empty pages – pages with no entries – shall be removed from the page sequence.

The Authority prefers that generalized filter (search) and sort commands are available on list displays. List searching shall include "Index", "Contents", and "Phonetic" search capabilities.

16.3.7 Scaling and Translation

Certain displays, such as power system overview displays, shall be based on world coordinate space. The user shall be able to scale the image of a world coordinate space or other display in a smooth fashion. Scaling (zooming) shall be possible by using mouse scroll wheel, buttons, rubber banding, hot keys, etc. The scale factors shall allow the presentation of an entire world coordinate space or other display on the full monitor or a window. 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. At defined scale factors, levels of declutter shall be invoked.

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. The window dimensions shall not be changed by such an action.

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. Static and dynamic data shall be displayed and updated during a translation operation.

16.3.8 Schematic and Geographic Display Interactions

Authority dispatchers shall have access to displays that show selected geographical and schematic world-map views of the Authority's power system. In this respect, visualization facilities shall be made available to make best use of these displays.

Typically, the dispatcher will work with the schematic rather than geographical world-map display to monitor and control the power system. On the other hand, it is desirable that the dispatcher, by simple

cursor operations, can quickly access the geographical world-map display corresponding to any selected view (i.e., portion) of the schematic world-map display and then interact with the geographical display in any way normally available to users of such displays. This includes, for example, panning and zooming, monitoring alarms, and implementing device control actions. The dispatcher should then be able to remove the geographical display from view and continue using the schematic display to support further monitoring and control activities.

In a similar fashion, it is also desirable that the dispatcher, when working with a geographical world-map display, can temporarily access and interact with the schematic world-map display starting from the schematic world-map view corresponding to the initial geographical world-map view.

16.3.9 Supervisory Control Initiation

Supervisory control actions shall be initiated through dialogs that present commands dependent on the type of element to be controlled. As the final step of the supervisory control process, 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”). The TDMS shall issue the command to the end device only after the user confirms the operation.

16.3.10 Data Entry

User entry of data, such as analog and status values as a substitute for telemetered values, 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. Data entry may use full window or single point techniques as appropriate.

The full window entry mode shall be initiated by user action and shall simultaneously affect all points on the display within the window for which data entry is possible. The TDMS shall respond by suspending the updating of the display and highlighting all points on the display that may be entered. The user shall then enter the new values and request entry of the values. The value appearing in the entry field shall be the value processed for entry into the database. The TDMS 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. 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.

The user shall initiate single-point data entry by selecting the point to be entered and commanding the data entry mode. Only the selected point shall be placed in the data entry mode. The remainder of the entry procedure shall be as for full-monitor entry.

Entered data, particularly free-format text fields, shall be checked to ensure that they contain only valid characters, do not contain embedded program codes, are of the proper format, and are within the expected length of the entered field.

16.3.11 User Action Recording

All user actions that change TDMS data or operating conditions shall be recorded as events, except for the following:

1) Actions that request displays or modify their presentation, such as scaling, translation, paging, scrolling, relocating windows, and resizing windows.

2) Execution of power system network analysis functions in study and simulation modes including data setup, execution setup, and execution.

Each event record shall include:

1) The login identity of the user.

2) The time and date of the action.

3) A complete identification of the database point affected.

4) A clear (non-coded) description of the action.

5) The value, state, or condition of the item changed before and after the action.

16.3.12 Interlocks

Although the same display may appear concurrently in multiple windows at multiple workstations, data entry for that display shall be restricted so that multiple users will not produce conflicting actions on a given value. If a display is in the full-window data entry mode in one window, an attempt to initiate the data entry function for that display in another window on the same or another workstation shall result in rejection of the second attempt to enter the data entry mode and the second user shall be informed of the conflict.

Similarly, control of a power system device, management of a single point (such as suspending data acquisition for a point), and single-point data entry shall only be allowed from one window at one workstation at a time. Concurrent user action on different areas of a world coordinate map or other display and concurrent supervisory control, data management, and single-point data entry of different points on the same display shall be allowed.

16.3.13 Memos

Users shall be able to define and attach memos to displays. These memos shall contain free-form text entered in Thai and/or English via the workstation keyboard. In addition, the user shall be provided with the capability to copy portions of applicable TDMS files containing text or graphics (such as diagrams and pictures) and paste these items into memos. After definition of the memo contents, the user shall have the capability to attach the memo to any location within a display. A unique icon or indicator shall be used to visually highlight for the user that a memo is assigned to the display. The memo icon shall be visible at all declutter levels.

Memos shall be checked to ensure that they are within the allowed length of the entered field and contain only valid information that does not contain embedded program codes or instructions that could be inadvertently executed when the memos are displayed.

16.3.14 Field Crew Location

The TDMS shall support dynamic field crew location. Thus, it shall be possible for dispatchers to track field crews by viewing special symbols automatically placed on geographical power system displays.

The basis for field crew tracking shall be the Automatic Vehicle Location (AVL) function. This Contractor-provided function shall be able to receive geographical location signals (latitude and longitude coordinates) from Authority GPS master stations capable of receiving these signals from GPS receivers installed in the field crew vehicles by the Authority.

By selecting a symbol, crew ID, vehicle and equipment details, and other relevant information shall be displayed. In addition, it is desirable that the dispatcher shall be able to add information such as "on route", "at site", "on break", "work completed", "returning to depot."

The symbols shall be capable of distinguishing between the different field crews in a manner to be approved by the Authority. It shall also be possible for Dispatchers to manually place or move the symbols in the event, for example, the automatic placement function becomes inoperable.

Based on vehicle location, additional features shall be considered by means of which Dispatchers can visualize the work that the crew is performing. This may be supported, for example, by views of crew surroundings such as those available via Google Earth or from videos and photographs downloaded to the TDMS from field crew tablets and mobile phones connected to the Corporate WAN. Within this context, the Contractor's proposal shall have described all enhanced visualization capabilities and features that may be supported.

16.3.15 Jumpers, Grounds, and Cuts

Users shall be able to apply jumpers, grounds, and cuts to power system displays to reflect temporary changes such as repairs that have been implemented in the field. As devices, they shall be treated as all other devices from the perspective, for example, of switching, tagging, topology, and coloring.

The temporary changes shall update the power system model without the need for any permanent change requiring regeneration of the TDMS database. Application shall be accomplished easily using special symbols approved by the Authority. Removal of jumpers, grounds, and cuts shall be accomplished just as easily to reflect completion of the repair work and quickly return the power system model and display to their original states.

To support this temporary change capability, a special "Temporary Change Summary" display shall be provided. This display shall list each change as a time-stamped event.

16.3.16 Equipment Information

On power system displays, it shall be possible for the user to point and click on equipment and have the TDMS respond by presenting stored information related to this equipment. The information may include, for example, a photographic image and/or drawing of the equipment along with nameplate, configuration, and other details including the equipment's maintenance, outage, and operating history.

It shall also be possible to access every attribute of the selected equipment, or selected data point, in order to dynamically control the appearance of the equipment and data points wherever they may be shown within the TDMS display subsystem. This shall include the capability to control the presence, appearance, and location of associated quality codes, e.g., to control whether all applicable codes or only the one with the highest importance is to be shown.

16.3.17 Inactivity Timeout

The progress of all user operations shall be monitored. 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. A partially completed action shall be reset if the user begins another non-related sequence.

A second inactivity timeout, constrained to be no shorter than the above timeout, shall blank the monitor upon timeout. Any user activity, including keyboard or mouse actions, shall bring the display on view immediately prior to the timeout back to view.

16.3.18 User Guidance

The TDMS shall respond to all user actions indicating whether the action was accepted, was not accepted, or is pending. For multi-step procedures, the TDMS shall provide feedback at each step. Indications such as text messages, color changes, and blinking shall provide this feedback.

16.3.19 User Help

General and specific context-sensitive on-line help shall be available to the TDMS user. Access to user help shall be available by:

1) A Help command on the window menu bar.

2) A Help button in a dialog box.

3) Topics from a Help menu.

Using Thai and/or English, the Help menu shall present a list of topics available for reference. The topics shall refer to the TDMS user documents. The ability to scroll through the topic's explanatory text shall be supported.

The Help button in a dialog box shall present the text of the TDMS user documents where use of the dialog box is explained. 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.

As a minimum, context-sensitive help facilities shall be provided for each application software package and the database fields.

No external network access shall be required to access any necessary help or support documentation, such as an operations manual. Help documents shall be free of any embedded virus or other mal-ware codes.

The "Help" function's scope shall be sufficient to instruct the user on normal operation of the TDMS and its applications without resorting to a printed user's manual. The appearance and capabilities of the help function shall be like those of the help function provided with Microsoft Office, including the feature where selection topics are suggested based on a partial or complete search string entered by the user. With a single mouse click on any display, the user shall be able to access a help window that explains every pushbutton, pull down or dialog menu, and data field associated with the display. Possible error messages associated with operations available from the display shall also be explained. The "Help" window shall remain on the monitor until it is closed by the user, or until the display from which it was called is replaced.

The capability to easily edit or add additional help facilities shall be provided. Thus, in addition to the above, for example, the TDMS shall include tools enabling the user to edit and add to the "Help" text, including the associated operations manuals and monitors.

16.3.20 TDMS Access Security

A mechanism for defining and controlling user access to the TDMS shall be provided. This security scheme shall be in addition to that included with the operating system. That is, even though a user has logged onto the TDMS network or a processor, access to the TDMS functionality shall be subject to additional security checks.

16.3.20.1 User Login

Password security shall be provided for access to the TDMS. 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. TDMS passwords shall be encrypted at the workstations and transmitted over the network and stored in encrypted form. It shall not be reasonably possible to reconstruct a password from the stored encrypted value.

Within this context, the TDMS shall enforce the following password construction rules recognizing, however, that the system administrator may configure them on an individual basis to be enabled or disabled:

1) Configurable minimum length (initially set to 7 characters).

2) Mandatory inclusion of alphabetic (upper and lower case), numeric, and, possibly, "special" (non-alphabetic or numeric) characters.

3) The password shall not be the same as the user ID.

4) The password shall be required to be changed periodically, initially every 90 days (adjustable), not more often than once per day.

5) Simple pattern changes (e.g., "Sdef78" changed to "Sdef79") shall be prohibited.

6) Previously used passwords shall not be reused.

Users shall be able to change their own passwords. Changed password shall be propagated throughout the TDMS as necessary and without additional user intervention. An appropriately authorized user may administratively reset passwords. Administratively reset and expired passwords must be changed at the next login.

16.3.20.2 Access Security Management

The cyber security features shall be consistent across all TDMS applications and services and security shall be managed as a single service for all component systems of the TDMS.

The TDMS shall record all attempts to access the TDMS both at the application level and at the "infrastructure" (operating system and application support software) level. The record shall include:

1) All attempts to log on, whether successful or unsuccessful.

2) All changes to privileges assigned to users and to workstations.

3) All user actions affecting security, such as changing passwords.

4) Attempts to access a file for which the user has no access privileges.

5) Attempts to perform an action not authorized by the security scheme.

For the purposes of the above requirements, the term "user" shall refer both to human users and to applications requesting such actions.

All access records shall be stored within the TDMS on auxiliary memory. 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. 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. The access-security recording scheme shall include a feature to archive the record file and to direct the records to a new, empty file.

The TDMS shall generate an alarm when access activity may be indicative of attempts to obtain unauthorized access to system services or data. A simple method shall be provided for the user to view and to change the rules for generating alarms. Initially, an alarm shall be generated when the system detects the any of following activities:

1) Repeated attempts from a specific workstation or external port to log in.

2) Repeated failed attempts at file access.

3) An unusually high frequency of supervisory control activity.

4) Port scans (attempts to access closed ports or services).

5) Unusual levels of traffic on the local area network.

The delivered TDMS shall not include any guest accounts or default administrator or maintenance accounts providing user access. It shall not include any accounts that do not require an interactive log in. All accounts in the delivered TDMS shall use passwords assigned by the Authority.

16.3.21 Areas of Responsibility

Once logged on, access to the TDMS capabilities shall be managed by assigning Areas of Responsibility (AORs) to each user account. There shall be no restrictions on the assignment of multiple AORs to a user.

Each AOR assignment shall be further defined as either read-only or read/write. Read-only access shall preclude user interaction with the display other than to request another display. Read/write access shall allow full interaction with the display subject to the AOR's function, database, and supervisory control limitations.

The access security validation procedure shall follow a hierarchy of AORs:

1) *Displays* – Each display shall be assigned to a single AOR. The presentation of each display shall be limited to users assigned to that AOR, even though access to the functions, data items, or supervisory control devices presented on the display may be allowed.

2) *Functions* – Each function shall be assigned to a single AOR. Access to the facilities of any function shall be limited to selected users even though access may be permitted to a display from which such facilities could be exercised. The means by which displays, reports, and databases are defined and modified shall be considered functions, as well as functions that manage the software configuration of the TDMS. These functions shall be subject to the same access security validation as other functions. Management of AORs shall be a function itself subject to validation.

3) *Database Items* –Each database item shall be assigned to a single AOR. Attempts to manage any database item shall be denied if the item's AOR does not match the user's AORs. Database item management regulated by the operating AOR scheme shall include:

    a) Enabling and suspending acquisition, calculation, and processing.

    b) Inhibiting and enabling alarm processing.

    c) Manually substituting a value.

    d) Overriding a limit.

    e) Managing alarms, including alarm acknowledgement and deletion.

4) *Supervisory Control Devices* – Each database item for which supervisory control has been defined shall be assigned to an AOR. Attempts to initiate supervisory control actions shall be denied if the supervisory control database item's AOR does not match the user's assigned AORs. Access to supervisory control facilities shall encompass not only control, but also

access to the control inhibit (tagging) feature for the database item. Control of the TDMS hardware configuration shall be considered a supervisory control procedure.

The access security function shall ensure that each AOR is always assigned to at least one user. If a reassignment of AORs results in one or more AORs not being assigned to at least one user, the unassigned AORs shall be automatically assigned to a pre-assigned user and suitable alarms shall be generated.

16.3.22 Advanced Visualization Features

Advanced Visualization tools shall be provided to enhance situational awareness. These features shall include dynamic dashboards, dynamic color contouring, 3D objects, and animated objects.

Dynamic color contouring shall be configurable to show variations in color or intensity to depict menu driven system values or limit conditions from real-time data. Contouring techniques shall be capable of being applied to voltage levels, line real and reactive power flows, and power flow injection and withdrawal points.

Dynamic dashboards shall be provided. Dashboard displays shall represent a configurable window by each user representing a simultaneous view of data and displays from multiple sources in the system including real-time, study or historical data as well as alarms and alarm counts. Displays shall be user configurable with drag and drop techniques from any existing graphic, tabular or trend display. Dashboards shall be user configurable by the dispatcher. They shall have the capability to drill down, provide the ability to use hyperlinks and pop-ups, and can include animated objects.

Display objects including cylinders, cones, etc. shall enable the user to depict system conditions of interest on select 3D displays.

Display objects including animated arrows or other graphic symbols shall be configurable by the user to depict specific conditions for individual system elements of interest. Animation features shall enable the user to define dynamic sizing, direction, color and object speed for individual value conditions such as showing arrows to show real and reactive power flow, halos for violations, increasing line size for limit violations, etc. The user shall be able to disable and enable any animation feature via on-screen menus.

Dynamic characteristics from the Real-Time Database (RTDB) shall be capable of being displayed with coloring and gradient effects to reflect the dynamic state of the network. As violations occur, the coloring shall identify this.

All groupings, colors, and dynamic behavior related to the presentation of the above features shall be configurable by the Authority and will not require any customization on the part of the Contractor.

16.3.23 Data Access Spreadsheet

A spreadsheet application shall be included in the TDMS to enable users to perform ad-hoc calculations and to define more permanent calculations and format them for viewing and printing. The intent is to

allow the Authority to use spreadsheets as TDMS displays to present user-specific calculated information. Incorporation of a commercially available spreadsheet such as Excel is preferred.

In addition to manually entering variables into the spreadsheet, it shall be possible to copy values from the TDMS databases. Thus, the following general capabilities are required:

1) Interfaces and methods for easy retrieval of historical data into spreadsheets.

2) Linking of spreadsheets to the RTDB.

Methods shall include drag/drop and copy/paste techniques. Clicking a Refresh button shall cause all the values derived from databases to be updated and a recalculation to be performed.

16.4 Alarm and Event Processing

Alarms are conditions that are annunciated to users when detected and that require user action. Alarms may be generated by any TDMS function. When initially detected, they shall be marked as "unacknowledged." Users will indicate that they have acted on the alarm by acknowledging the alarm.

Events are conditions that are to be recorded by the TDMS, but that do not require annunciation or action, including acknowledgement, by users. Events may be generated by the same functions as alarms. Events may be considered as special cases of alarms, where the event is intended only to record information.

Alarms shall be subjected to a series of alarm processing actions and user interactions. The actions to be executed shall be determined by the AOR assigned to the database item that is exhibiting the alarm condition and by the alarm class that is also assigned to the database item.

Each database item may be associated with several alarms. For example, a telemetered analog point will include operating limit alarms, reasonability limit alarms, and telemetry failure alarms. Each alarm of each point shall be individually assigned to an AOR and to an alarm class.

16.4.1 Alarm Class and Alarm Presentation

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

1) Audible annunciation – single stroke or repeating and tone to be sounded.

2) Display presentation:

    a) For one-line diagrams – symbol change, color change, or no change, and flash/no flash for unacknowledged alarms.

    b) For message displays (such as an alarm summary) – message color and flash/no flash.

3) Inclusion on or exclusion from the alarm window.

4) Inclusion on or exclusion from the alarm summary (all alarms and events shall be included on the event summary).

5) Alarm management (acknowledge and delete):

    a) None required (for events).

    b) Acknowledgement is required before deletion.

        i) Manual deletion (user action) is required.

        ii) The alarms are deleted when the return-to-normal alarm for the point is acknowledged.

        iii) The alarms are deleted when the alarm is acknowledged.

    c) Acknowledgement is not required before deletion. Unacknowledged alarms may be deleted.

        i) Manual deletion (user action) is required.

        ii) The alarms are deleted when the return-to-normal alarm for the point is acknowledged.

        iii) The alarms are deleted when the alarm is acknowledged.

16.4.2 Alarm Messages

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

1) The time and date of the alarm (with alarms from previous days clearly identified)

2) A complete identification of the database point

3) A substation or feeder code name (defined by the Authority)

4) A clear (non-coded) description of the alarm

5) The value, state, or condition of the item changed before and after the alarm.

The alarm message shall be unabbreviated English and/or Thai text and shall not require the use of a reference document for interpretation. The Authority shall be able to modify alarm message formats and define new formats.

16.4.3 Alarm Window

The alarm window shall provide a visual indication of alarm conditions in every AOR assigned to the workstation user. The alarm window shall contain an indicator for each data source and each TDMS

function. Indicators for data sources and functions with no alarm conditions present shall not be visible. 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. Acknowledgement of the alarm shall modify the attributes of the indicator to indicate the presence of only unacknowledged alarms.

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

16.4.4 Alarm Acknowledgement

The user shall be able to acknowledge alarms associated with any application or database condition on any display that presents the alarm. Alarms shall also be alarmed programmatically. 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.

Alarms shall be acknowledged both individually and in multiples. Individual alarm acknowledgement shall require selection of a specific alarm before the acknowledgement is commanded. 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.

Page acknowledgement shall be supported only on the alarm summary display and shall affect only those alarms visible within the window at the time the acknowledge action is commanded. It shall not be possible to acknowledge alarms that are not in the view of the user at the time of the acknowledge action. The TDMS shall operate successively on each message selected for page acknowledgement.

16.4.5 Alarm Deletion

The user shall be able to delete alarms associated with any application or database condition on any display that presents the alarm. Alarms shall also be deleted programmatically. 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. However, all other alarm attributes shall remain as they were before the delete action and the alarm conditions shall continue to be shown on displays other than the alarm summary.

Alarms shall be deleted both individually and in multiples. Individual alarm deletion shall require selection of a specific alarm before the deletion is commanded. If an individual point in alarm is selected on the alarm summary display, the deletion action shall affect only that message. If an individual point in alarm is selected on any other display, the deletion action shall affect all alarms for that point.

Page deletion shall be supported only on the alarm summary display and shall affect only those alarms visible within the window at the time the deletion action is commanded. It shall not be possible to delete alarms that are not in the view of the user at the time of the deletion action. The TDMS shall operate successively on each message selected for page deletion.

16.4.6 Alarm Inhibit and Enable

Alarm annunciation for any point shall be inhibited and enabled by user command. 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. However, the point in alarm shall be marked as unacknowledged and any alarms detected shall not be annunciated or presented on the alarm summary. Alarm conditions and messages existing at the time of an inhibit action shall remain as they were before the action. Alarms detected after an inhibit action shall not be annunciated when alarming is enabled.

16.4.7 Alarm Audible Silencing and Suppression

Audible alarm annunciation shall be silenced, suppressed, and enabled by user command. Alarm audible silencing and enable operations shall be reported as events.

Audible alarm silencing shall stop ongoing audible annunciation at the workstation issuing the silence command. New alarms shall again sound the audible alarm.

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. 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.

16.4.8 Enhanced Alarm Management

Additional features for alarm management shall be provided. Desirable features of the enhanced alarm management function include:

1) Minimization of nuisance alarm messages (for example, repetitive alarms for the same alarm condition).

2) Combining of related alarm messages.

3) Prioritization of alarm messages.

4) Highlighting of the most urgent messages.

5) Suppression of alarms based on related alarm conditions.

6) Evaluation of related alarm conditions to determine the true alarm condition.

16.5 Display Hardcopy

The TDMS shall print a copy of a window on any workstation when commanded by a user. The output shall be directed to a printer of the user's choice. 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. 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.

16.6 User Interface Development

Tools to define and maintain displays shall be provided with the TDMS. The display "editor" shall support the definition of all of the displays in the TDMS and shall be the same tool used by the Contractor to develop displays provided by the Contractor.

16.6.1 Display Style

All displays provided by the Contractor shall have a consistent layout and consistent rules of operation (also known as a consistent "look and feel"). Each display shall 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 TDMS. This requirement shall apply to displays provided from the Contractor's standard offering and displays developed specifically for the Authority as part of this contract.

The Contractor shall submit a display style guide for Authority review and approval. All displays produced by the Contractor as part of their standard product shall comply with this guide. The display style guide shall take the Authority's existing display conventions and standards into consideration. At the Authority's option, any displays produced by the Contractor or the Authority, excluding displays to be incorporated into the Contractor's standard product, shall be produced in compliance with the Authority's display conventions and standards.

16.6.2 Display Generation and Editing

An interactive display generation and editing tool shall be provided for creating the operational displays and interfaces associated with each application. With this tool, the user shall draw (rather than code) the contents of application windows, define dynamic linkages to any TDMS data, and sensitize display elements to respond to user input actions (such sensitized elements are typically referred to as cursor targets and function keys). The ability to link to any TDMS data, not only real-time data, shall allow interactive graphic displays to be constructed for all applications in the TDMS via the display building tool.

The display editor shall be used to construct new displays and modify existing displays. The editor shall support displays constructed as world coordinate spaces and displays constructed as fixed spaces (displays built to a fixed coordinate space, which can be translated but not scaled).

The display editor shall be fully compatible with the database generation and editing function. The display editor shall be fully interactive and shall provide "What You See Is What You Get" (WYSIWYG) capabilities. The display editor shall maintain a complete audit trail of edit activity as part of software configuration management. New displays shall be constructed beginning from a blank display, from an existing display definition, or from display templates within a library. 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. The editor shall be designed such that any future display requirements may be readily added to its functional display definition capabilities.

The display editor shall support the listing, dumping, reloading, and validating of display definitions. The list function shall provide for partial and full summaries (directories) of displays cross-referenced

to their use in applications. The list function shall also produce detailed documentation of the contents of any display showing all elements. The list function shall also provide tools to find on which displays a given piece of data is referenced. Dumping and reloading of displays shall be provided for individual displays, display libraries, individual applications, or an entire application system.

The display editor shall produce displays compatible with every workstation of the TDMS. The Authority shall not have to develop multiple versions of displays for each type of workstation or for different GUI products included with the TDMS.

The display editor shall support, as a minimum, the following construction features:

1) Editing features to copy, move, delete and modify selected individual items and groups of information and to undo/redo the previous actions

2) Building a display at any scale (zoom) level

3) Visible and invisible snap-grids at specifiable increments with (selectable) snap-to-placement of objects on the grid

4) Various font sizes, line types, and line thickness

5) Linking of any defined graphics symbol to any database point

6) 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.

7) Ability to establish different symbol or display conventions for the same database point on the same or on different displays

8) Definition of dynamic display linkages to any TDMS database variable on any TDMS display

9) Building and modification of display icons and store them in an easily accessible library

10) Protection of any data field on any display against user entry based on log-on identifiers

11) Activation of displays within any application system or across all application systems by a simple procedure that causes no noticeable interruption of on-line TDMS activity

12) A scripting tool to facilitate the modification of displays to incorporate Authority changes on top of any Contractor product upgrades and to port existing Authority displays and third party products into the Contractor’s system

13) Using geographical display information imported from the Authority’s GIS to initially create power system geographical displays and subsequently update them on an incremental basis.

14) Using AutoCAD drawing files as input. Such files shall be directed to specific layers of a world coordinate display where they shall become static display elements.

16.6.3 Display Elements

Displays shall be composed of the following display elements:

1) Text.

2) Drawing primitives (polylines, polygons, arcs, circles, ellipses, etc.).

3) Bit-mapped images.

4) Formatted data items.

5) Display macros.

6) Display layers.

7) User interaction features.

8) Display Libraries.

Drawing primitives and text shall refer to common graphic attribute definitions for color, line width, fill pattern, etc. Text shall also refer to fonts.

16.6.3.1 Data Presentation

The user, during the interactive display definition process, shall logically identify individual dynamic data fields and data arrays in defined displays. 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. The linkages between the displays and the database shall be by logical identification (for example, point name or point identifier) and shall be designed such that any database modifications (even those resulting in insertions into tables/files and changes in table/file sizes) do not require redefinition of existing displays.

Data fields shall reference all supported formats. 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 TDMS context. Formats shall be conveniently definable and modifiable.

It shall be possible to present any item in the database on any display. Database items shall be displayable anywhere on the monitor, excluding dedicated monitor areas such as the display heading. There shall be no limitation on the number of data items presented on any display, up to the physical limitations of the window or monitor. Similarly, monitor locations for cursor targets shall be unrestricted.

Database items shall be presented in the following formats as appropriate:

1) 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.

2) Symbols, including alphanumeric text strings for a single item, based upon the item's state for all defined states.

3) 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).

4) X-Y and X-t point relationships with vectors connecting the points, e.g., trending and Kiviat plots.

5) Filled polygons (x or y axis inside the polygon showing the percent of full scale of the variable); for example, bar charts.

6) Filled arcs; for example, pie charts or simulations of meter movements.

7) Colors, textures, and blink conditions based upon state or value changes or a change of data quality; for example, alarm limits.

8) Combinations of the actions listed above; for example, change a bar chart color when the data value exceeds the limit.

16.6.3.2 Quality Code and Tag Presentation

The quality code reflects the condition of the data on the display. When more than one condition applies to the data, the highest priority condition, as determined by an Authority defined priority sequence shall be displayed. The Authority shall determine the presentation of each quality code. Color, appended symbols, and other display features may be used. 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.

A separate indicator shall be used to reflect the tag status of a database point. When more than one tag applies to a point, the highest priority tag, as determined by an Authority defined priority sequence, shall be displayed. The Authority shall determine the presentation of each tag. Color, appended symbols, and other display features may be used. It shall be possible to construct multiple representations for a data item and its tags such that the presentation of data may be optimized.

16.6.3.3 Data Sets

Selected displays will be defined with the intent of presenting data from different "data sets." A data set is, for the purposes of this requirement, 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.

Data sets from different TDMS applications include data for the same power system devices. Some examples are as follows:

1) SCADA – the real-time measurement set.

2) Distribution State Estimation - the current real-time solution.

3) Distribution Power Flow – one or more study cases.

It shall only be necessary 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.

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, for example, to uniquely highlight the data generated by SCADA, Distribution State Estimation, and Distribution Power Flow.

Called displays shall default to the real-time data set. However, display requests 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. Displays defined to present multiple data sets shall clearly indicate the data set being presented. Data set identification shall be unambiguous, obvious, and visible at all times.

16.6.3.4 Display Macros

Macros form an arbitrarily complex hierarchy of display elements, primitives, symbols, and other macros. Display macros shall be created with an editor designed for this purpose. It shall be convenient to switch back and forth between macro editing and display editing. The editor shall support an arbitrary number of sharable macro libraries. Changes made to macros shall automatically be reflected in all displays that use the macro once the macro is installed in a system.

Display macros shall be placed individually. The user shall be prompted for necessary additional information as required by the macro. For instance, if the macro references a field of a certain record type, the macro placement shall prompt the user to identify which record is being referenced.

For all record references, it shall be possible to supply the required reference by selecting it with the cursor from any list or from another macro placement showing the record in any window at the workstation. A generalized copy/paste facility for data references is preferred.

16.6.3.5 Display Layers

World coordinate displays shall be constructed in layers. Each layer shall be a self-contained world co-ordinate space onto which display elements, including data, shall be placed. Layers shall be displayed in a defined order, with higher-order layers overlaying lower-order layers. Where displayable elements of a multiple layers occupy the same space, the higher-order layer elements shall be displayed. Otherwise, the elements of the lower-order layers shall be visible.

The selective presentation of layers – “decluttering” – shall be controlled by the scale (zoom) level and by user selection. Each layer shall be visible over a range of scale level set defined as the display is built. As the user scales the display, layers shall be presented or removed from presentation. It shall also be possible for the user to override the automatic selection of layers and to select those layers presented at any time.

16.6.3.6 User Interaction

Cursor targets shall send a message to an application or issue a command when events (such as a user action) occur. The TDMS shall support the following commands via user interaction:

1) Call a display (in the window of the calling command or in a new window as defined for the command). 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.

2) Initiate a program (a TDMS application, operating system, utility, or third-party program).

Such commands shall convey both fixed and contextual data. As a minimum, supported contextual information shall include:

1) Record identities linked to the cursor target

2) Cursor position on the monitor and within the display

3) Database, application, and application system associated with the display

4) List position (for lists)

5) Workstation identification and any associated parameters, such as AORs.

Conditional attribute values shall be attached to any display element, primitive, or macro. Conditional attributes 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. 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. Other examples of some of the attributes of power system entities that can be color-coded are states (in service/out of service/manually overridden, etc.) and values (real time, state estimated, unavailable, good, bad, manually overridden, etc.).

The TDMS shall support “pop-up” and “pull-down” menus for user interaction. Those menus supplied with the TDMS shall be extensible by the Authority to incorporate new features and applications developed by the Authority. 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. The menu items, when selected, shall pass messages to applications including fixed and contextual data as described above.

16.7 Display Types

The Contractor shall be responsible for providing all TDMS displays. As a minimum, the display types described below shall be provided.

16.7.1 Power System World-Map Displays

World coordinate displays showing geographical and schematic views of the Authority’s power system shall be provided. As background, these displays shall be capable of being supported by Google Maps

or their equivalent. As a minimum, the elements of the power system shall include generators, substations, transformers, circuit breakers, line reclosers, switches, disconnects, reactors, capacitors, feeders, line recloser/regulators, Var controllers, feeder remote controlled switches, fuses, and customer service drops.

Telemetered and calculated data shall be presented on these world-map displays. Flows such as Amperes, Watts, and Vars shall be displayed as values with direction arrows. In addition, the symbols used to represent the elements of the power system shall reflect the presence of alarms and other abnormal operating conditions. This shall include the use of highlighting to distinguish elements that have exceeded loading limits and different colors to distinguish elements that have been de-energized.

The display of information such as power quality violations received from MDMS Smart Meter reads shall also be supported.

Panning and zooming and other convenient means of navigating within the geographical and schematic world-map displays shall be provided. The user, for example, shall be able to navigate to substation one-line displays by selecting poke points on the world-map displays. In addition, to navigate to specific power system equipment or data point locations within a world-map display, the capability of the user to do this by user defined criteria such as substation name, feeder name, operation ID, or point name shall be provided.

The user shall be able to interact with the world-map displays to enter data, attach memos and field crew symbols, apply temporary jumpers, grounds, and cuts, select equipment to access related information, and perform supervisory control, etc.

16.7.2 Substation One-Line Displays

Substation one-line displays show the interconnected elements of individual substations. The elements shall include buses, incoming and outgoing lines, transformer banks, circuit breakers, line reclosers, capacitor banks, and disconnects, etc. The displays shall present telemetered and calculated data, including all alarm conditions. Highlighting and colors used to distinguish the operating states of the different substation elements shall be consistent with all other one-line displays. 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.

The user shall be able to navigate to other substation displays from poke points on transmission line segments on the one-line. The user shall also be able to call-up the associated substation tabular display from a poke point on the one-line.

16.7.3 Other One-Line Displays

Other one-line displays may be provided to show the power system to the Dispatcher. For example, one-line displays may be provided of major sub-transmission and distribution circuits. The characteristics of these displays shall be the same as the power system world-map displays and the substation one-line displays.

16.7.4 Substation Tabular

Substation tabular displays list the value of telemetered and calculated data associated with each substation as well as related information such as alarm limits. The user shall be able to interact with the substation tabular displays to perform any associated user interactions such as data entry and supervisory control. The user shall be able to call-up the associated substation one-line display from a poke point located on the tabular display.

These displays shall be generated automatically by the TDMS upon call up and shall be based on the current contents of the database. The Authority shall have approval over the format of these as well as other displays. Points displayed shall be all database points within the substation:

1) *For status points* – The information displayed for each point shall include:

    a) Name descriptors.

    b) All data attributes.

    c) Current status.

    d) Normal status.

    e) Quality codes and tags.

2) *For analog points* – Information displayed for each point shall include:

    a) Name descriptors.

    b) All data attributes.

    c) Current value.

    d) All limit values.

    e) Quality codes.

3) *For accumulator points* – Information displayed for each point shall include:

    a) Name descriptors.

    b) All data attributes.

    c) Current value.

    d) Quality codes.

The types of point shall be displayed separately from each other and telemetered data displayed separately from calculated data. As many display pages as needed to show all points at a substation

shall be provided. 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.

16.7.5 Power Quality Tabular

These displays shall list the power quality data associated with customers. This data shall be based on Smart Meter reads that the TDMS receives from the Authority's MDMS or AMI Head-End Systems (HESs). Related information such as alarm limit violations shall also be listed. The user shall be able to interact with the tabular displays to perform any associated user interactions such as data entry and supervisory control.

16.7.6 Other Tabular Displays

Other tabular displays that contain telemetered and calculated data may be associated with Contractor or Authority-provided application programs. Tabular displays of power system circuits shall be included. 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.

16.7.7 One-Line Menu

These displays shall provide one-line menus for substations and power system circuits. Each entry in a menu shall allow selection of the associated one-line display. Entries shall be listed in a logical order approved by the Authority, e.g., entries for substation one-lines by name, entries for circuit one-lines by substation name and voltage class.

16.7.8 Access Control Display

This display shall allow designated and properly authorized personnel to control user access to the TDMS such as enter, modify, and delete user IDs and passwords and to assign workstation AORs and operating modes.

16.7.9 Menu Directory Display

This display shall list all menu displays in alphabetical order. Each entry in the list shall have a cursor target for menu selection.

16.7.10 TDMS Directory Display

This display shall list all TDMS displays in alphabetical order. Each entry in the list shall have a cursor target for display selection.

16.7.11 TDMS Configuration Monitoring and Control

These displays shall allow the user to monitor and control the TDMS configuration. The displays shall:

1) Present all equipment and communication link status and associated alarms.

2) Provide menus or cursor targets for performing actions such as failover, switching local and remote devices (such as workstations, servers, and field device interfaces), switching communication channels, controlling the TDMS resource monitoring function.

3) Present processor and communication channel loading and error statistics.

These displays shall graphically show the interconnected elements of the TDMS including communication paths and Contractor-provided channel interface equipment such as modems, transceivers, and multiplexers. The data sources, such as field device interfaces and other computer systems, communicating over each path shall be shown as well.

16.7.12 Summary Displays

Summary displays shall present power system and TDMS conditions. Unless indicated otherwise in the following specific requirements for individual summary displays, user interaction with the displays shall be limited to filtering and sorting the data presented in the displays. The TDMS shall support filtering by:

1) AOR.

2) Location (e.g., substation or feeder).

3) Point name.

4) Alarm class.

5) Date and time.

The TDMS shall support "wildcard" filters. The TDMS shall support sorting in both increasing and decreasing alphanumeric as well as date and time directions. At least three concurrent filters, each with sorting, shall be supported.

It shall be possible to define default filters and sorting for summary displays such as follows:

1) 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.

2) All other summaries – sorted by location (alphanumeric) and then by date and time. No filter shall be applied. The summaries shall be filtered to present only the entries corresponding to the user's assigned AORs.

16.7.12.1 Alarm Summary

A single user action shall be used to call an alarm summary that presents only those alarms for the AORs assigned to the user. All alarms in all classes shall be presented. The TDMS shall also include facilities to call a general alarm summary, with a single user action, that will present all alarms in all AORs.

Alarm summaries shall show power system and TDMS alarms. The user shall be able to acknowledge and delete messages on the display. Flashing shall identify unacknowledged alarms. To facilitate reading unacknowledged messages, only the time field shall flash. The alarm class shall determine the response of the TDMS to acknowledge or delete actions and to annunciation of return-to-normal alarms.

The Authority prefers an implementation where the alarm summaries expand to display any quantity of alarms. 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. It shall be possible to perform any alarm interaction from the alarm summary displays.

Furthermore, a quick locate function shall be provided such that the user via a single click of the cursor can navigate from any active alarm entry on the alarm summary display to the one-line display, and (as may be desired) to that part of the power system world-map display, where the alarm condition shall also be presented.

16.7.12.2 Event Summary

The event summary shall be similar to the alarm summary with the exception that all alarms and events (such as supervisory control commands, tag placement, and data management actions) shall be listed. Events shall be removed from the event summary only when the capacity of the display is exceeded. The oldest events shall be removed as new events are listed.

16.7.12.3 Off-Normal Summary

This display shall list devices and values that are not in their normal state. Telemetered, calculated, and manually entered status, analog, and accumulator data points shall be included. The displays shall show the off-normal data points in the following groups:

1) Status points for which the present telemetered state is different from the normal state stored in the database.

2) Analog and accumulator points that present values exceeding alarm limits.

16.7.12.4 Off-Scan Summary

This display shall list all points that have been suspended from acquisition.

16.7.12.5 SOE Summary

This display shall list SOE information retrieved from the IS&R function.

16.7.12.6 Alarm Inhibit and Override Summary

This display shall list devices and data values for which the user has inhibited alarm processing and for devices and data values for which the user has overridden limits. The entries for overridden limits shall show the database (non-overridden) value of the limit as well as the overriding value. Controls to enable sorting by substation and by date and time of the entry of the alarm inhibit or override shall be included on the display.

16.7.12.7 Tag Summary

This display shall list and describe all active tags for all devices. The user shall be able to place and remove tags from this summary. Information on this display shall list each device tagged and shall include:

1) Date and time of tag placement.

2) User who placed the tag.

3) Tag level.

4) Station identifier.

5) Device identifier.

6) Comment field.

16.7.12.8 Manual Replace Summary

This display shall list all points that have been replaced by manual entries. 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.

16.7.12.9 Temporary Change Summary Display

The Temporary Change Summary display shall list and describe each and every temporary change to the power system model as introduced by the user on one-line displays (such as power system world-map displays) to reflect, for example, field crew activities associated with the actual power system such as the application of jumpers, cuts, and grounds.

The temporary changes shall appear as events time-stamped by the TDMS at the time the user applies a jumper, cut, or ground on a one-line display. Subsequently, when the user removes the jumper, cut, or ground from this display, the corresponding entry in the Temporary Change Summary display shall be automatically removed as well. Another requirement relates to the capability of a user to click on any entry on the Temporary Change Summary to navigate immediately to the location of the temporary change as it appears symbolically on the power system geographical and schematic world-map displays.

16.7.13 Communication Maintenance Displays

Communications with data sources and other computer systems shall be managed via communication maintenance displays. These displays shall show the status of communication channels. Error counts and tabulations of all types of communication errors shall also be displayed.

16.7.14 Application Program Displays

The Contractor shall provide all displays associated with all specified application programs and functions. Displays that allow the user to interact with TDMS application programs shall use a common look-and-feel approach. The information provided shall help expedite the user's interactions.

16.8 Trend Displays

Trend displays shall provide the capability of TDMS users to view telemetered and calculated real-time data plotted against time in a horizontally or vertically oriented graph. In the trend displays, 1 (one) axis shall be time and the other axis shall be the value of one or more selected points as they vary with time. To support external users, properly authenticated, it shall also be possible to access trends as a Web service, i.e., by means of the Web Server to be provided in the DMZ as part of each data center's TDMS configuration.

16.8.1 Trending Capabilities

It shall be possible to select any analog point for temporary real time trending. It shall also be possible to assign any point to permanent trending. The values of permanently trended points shall be available in the historical database at time intervals that are commensurate with the scaling of the trending curve in such a way that at least 1 (one) value is saved for each pixel of the curve. For such points, (1) all the data needed for the curve shall be available whenever their trending is requested, and a complete curve shall immediately be displayed, and (2) it shall be possible to request trending of historical data for any period for which it is on-line.

The following trending capabilities shall be provided:

1) It shall be possible to define, separately for each trend display, horizontal or vertical orientation of the trending curves. For horizontally oriented curves, the value of time shall increase to the right (i.e., the oldest data shall be on the left and the most recent data on the right.) For vertically oriented curves, the value of time shall increase downward.

2) It shall be possible to plot at least 4 (four) curves, corresponding to 4 (four) separate data values, together on the same set of axes, and to define different scaling for each curve. All curves shown simultaneously on the same axes shall have the same time scale.

3) It shall be possible to select time scaling so that the complete (full-scale) time axis represents any user-selected period, such as:

    a) 1 (one) second

    b) 10 (ten) seconds

    c) 15 (fifteen) minutes

    d) 12 (twelve) hours

    e) 24 (twenty-four) hours

4) When several values from a trending file correspond to a single point on the trending curve, then the average trending file values shall be used to construct a point on the curve.

5) It shall be possible to select different time and value scaling for curves in different windows.

6) It shall be possible to define a unique color for each curve.

7) Using different colors, it shall be possible to identify portions of a curve that represent values marked with a “Failed” or “Deactivated” data quality, and manually entered values.

8) It shall be possible to assign a pair of limits for each curve and to select shading to emphasize the areas inside and outside the limits. For real time values the limits shall be linked, as a default, to the first, innermost, pair of operational limits of the trended point, but it shall also be possible to assign them to the point’s other pairs of operational limits, or to assign to each limit a value within the range of values of the trending curves. Only the last option is required for historical trends. The limits shall be shown as lines on the curve, and their numerical values shall also be shown.

9) It shall be possible to superimpose trend curves where 1 (one) curve represents historical data from a given period and the other curve represents the real-time data of the corresponding current period. (For example, a window might present two curves, one showing the load of a transformer on the day of the peak, and the other showing the current day's load, updated in real-time)

10) Trend curves for real-time data shall automatically be updated when a new value becomes available. When historical data for a corresponding period is superimposed on real time data, it shall be updated too in synchronism with the real-time data.

11) For trend curves showing real-time data, the position of the axes shall remain fixed, and the curves, time axis markers, and the grid shall move with the addition of newly acquired data.

12) It shall be possible to use a pre-existing trend curve as a template for a new trend curve by calling it up and then saving it under a new name or ID. This new trend curve can be modified by selecting different data points or other parameters.

13) It shall be possible to select historical data to be displayed in two ways: (1) static display of data for a user-specified period, or (2) dynamic display of as many of the most recent values as can be accommodated in the trend curve. Dynamic historical trends shall be automatically updated as new values are received.

16.8.2 Precise Reading of Curve Values

Users shall obtain a precise reading of values of each curve within the set of axes, at any point along the time axis, by placing a hairline cursor at the desired point. The time for which the accurate values are shown, and the engineering values of the curves corresponding to this time shall be shown. The user shall be able to quickly place the hairline cursor at any point on the curve and then move it slowly to precisely select the desired point.

When a new trending display is shown, the hairline cursor shall be placed at the end of the curve, so that the value of each curve is shown.

16.8.3 Selection of Trending Data and Parameters

It shall be possible to select any telemetered or calculated value for trending. For the selection of data for trending, a procedure is required which is based on pointing the cursor to the desired point; it shall not be necessary to enter a point name or ID to select a point for trending.

16.8.3.1 Pre-Selected Trending Points

It shall be possible to pre-select points for trending. Pre-select trending is also referred to as "permanent trending."

The momentary values of such pre-selected trending points shall be saved in the historical database at time intervals that are commensurate with the scaling of the trending curve in such a way that at least one value is saved for each point of the 1,024 points of the curve. For such points, all the data needed for the curve will therefore be available whenever their trending is requested, and a complete curve shall immediately be displayed. It shall also be possible to trend historical data points from the data repository. In this respect, the requirements below for displaying historical curves and overlays apply.

Trending data shall be transferred into the data repository for long term keeping and archiving. Historical and restored archived trending data shall be accessible to the trending function from the repository.

16.8.3.2 Presentation of Trending Curves

The following basic capabilities for the presentation of trending curves shall be provided:

1) When trending is requested for a point that is not assigned to permanent trending, the trend shall appear with system-wide, predefined, default trending parameters, including time and value scaling, default limits, and default shading attributes.

2) User shall be able to change all the trending parameters (scaling, limits, etc.) from within the display. This customized version shall apply only at the workstation at which it was prepared. A "Restore" function shall enable the user to request restoration of a permanent trend display to its assigned parameters or of a non-permanent trend to the default parameters.

3) A capability to buffer a user customized version for later recall is required for each trend display.

4) It shall be possible to select no less than 4 (four) points for trending within the same set of axes. It shall be possible to mix permanent trending points with non-permanent trending points.

For permanent trending points the user shall be able to request a curve of historical data to be overlaid on top of a curve of real-time data. The overlay shall be white with transparent shading through which the underlying curve is visible. The user shall be able to specify a date, whereupon data for the same

hours of the day shall be shown in the overlay. When real time curves get updated, the overlay curves shall likewise be updated with the corresponding values for the overlay date. The user shall be notified when historical data for the requested dates is not available.

16.9 Other Displays

Specific display requirements for other TDMS functions are described elsewhere in the Technical Specifications. The Contractor shall be responsible for the supply of all displays necessary to support the specified functions, in addition for any other TDMS displays required to control and monitor the TDMS itself. The Contractor's proposal shall have described these displays.

17. Hardware Requirements

This clause describes the minimum hardware requirements for the subsystems and equipment comprising the TDMS. In this respect, the Contractor shall be solely responsible for selecting, supplying, and integrating all necessary and sufficient hardware capable of meeting the Authority's overall TDMS requirements.

To the extent possible, the Contractor shall meet Authority requirements by providing hardware products available from local manufacturers or local OEM suppliers capable of providing full support for these products on a long-term basis, i.e., after the required warranty period has expired.

17.1 General Requirements

The hardware requirements are not meant to be restrictive. The Contractor shall have proposed hardware better suited to the characteristics of the Contractor's standard configuration if it represents a superior compromise between performance and cost. For example, blade rather than rack servers may be utilized. Any such hardware, however, shall not release the Contractor from the obligation to satisfy the functionality, availability, capacity, expandability, performance, security, and other requirements of the Technical Specifications.

All hardware shall be manufactured, fabricated, assembled, finished, and documented with workmanship of the highest production quality and shall conform to all applicable quality control standards of the original manufacturer and Contractor. All hardware components shall be new and suitable for the purposes specified. Within this context, the hardware shall have been accredited to quality standard ISO 9001, and all equipment shall utilize 230 VAC, 50 Hz as input power.

Delivered hardware shall include all engineering changes and field changes announced by the manufacturer since it was produced. The hardware shall be audited for change orders immediately prior to the factory performance test and unimplemented change orders shall be installed at that time. As part of the field performance test, the Contractor shall have all hardware inspected and certified as acceptable for service under a maintenance contract by the local service offices representing the equipment manufacturers.

17.2 Servers/Processors and Auxiliary Memory

All necessary servers/processors and auxiliary memory in support of the SCADA, IS&R, Network Analysis, Communications Network, Web Interface, and other TDMS functions shall be provided by the Contractor to satisfy the Authority's capacity, performance, and availability requirements. Based on the Contractor's optimal design approved by the Authority, virtual machine servers shall be utilized.

As a minimum, physical servers and processors shall be "x86" compatible and shall be based on a 64-bit, multi-core architecture with main memory, auxiliary memory, terminals, and all interconnections so that they can support data and information exchange (such as status and program or data control information).

All servers/processors shall be state-of-the art models selected for efficient operation of a real-time system. They shall include all necessary Client Access Licenses (CALs), and the latest security patches shall be installed. Generally, they shall be within the same model family. The Authority shall be able to replace or upgrade the servers/processors with future offerings to obtain increased computational power and system expansion with no required system or application software changes.

Each server/processor shall include facilities for orderly shutdown and resumption of operations upon detection of power loss and subsequent resumption of power.

No restrictions shall be placed on the allocation of server/processor main or auxiliary memory for any specific purpose.

Servers and processors shall be installed in rack mount enclosures provided by the Authority as part of each data center's infrastructure (refer to Clause 17.19.3). Minimum installation requirements are as follows:

1) Each rack shall include a 17-inch TFT color monitor, optical mouse, and keyboard as a server/processor and network management terminal. Monitor and keyboard shall be mounted for storage and ease of access using drawers of slide out type. The terminal shall manage all servers/processors in the rack via KVM (keyboard, video, and mouse) switches.

2) If not already installed by the Authority, an overhead extractor fan kit shall enhance natural convection cooling by increasing the airflow in the rack.

3) Grounding kit and any other necessary installation components shall be provided.

4) Equipment with a redundant power supply option shall be supplied with this option utilized.

5) All equipment with two network switching modules shall be configured to support No Single-Point of Failure (NSPOF). Necessary switches shall have a minimum interface speed of 1 Gbps.

6) Dedicated high-speed interconnections shall provide for efficient transfer of data to the system's Storage Area Network (SAN) and/or Network Attached Storage (NAS) infrastructure. These interconnections may be dedicated paths using Fiber Distributed Data

Interface (FDDI) technology for example or may be implemented on network paths shared with other servers and processors. All such interconnections shall comply with applicable international standards.

7) Server/processor auxiliary memory (NVMe preferred), including any RAID SSD units, shall be configured with a "hot-swap" maintenance capability. A hot spare SSD shall be included within any logical group of SSDs.

8) The servers/processors shall have warning lights that indicate and help identify equipment component or subsystem faults.

9) Redundant processors shall be housed in separate rack mount enclosures to enhance NSPOF capability.

10) Servers/processors equipped with dual Network Interface Cards (NICs) shall be configured so that their functionality shall be maintained if either or both NICs are connected to the network.

17.3 Front-End Processors

Front-End Processors (FEPs) shall be dedicated to TDMS data communications with all Field Device Interfaces (FDIs) except for the FDIs co-located with Switched Capacitor Banks (SCBs).

The FEPs shall check for and report protocol and other communication errors and convert the communications protocol to a common internal format compatible with the data processing functions of the TDMS. In this way, the FEPs can process the received data, in whole or in part, and store the processed data into the TDMS database or pass the data on to other TDMS resources for further processing (e.g., alarm annunciation) and storage into the database. To protect the security perimeter associated with the SCADA functionality of the TDMS, the FEPs may also serve as firewalls.

It shall be possible for maintenance engineers to monitor the performance of each communications circuit or channel, to enable and disable ports, and to switch to standby ports. Communications performance statistics shall be collected and presented in a form designed to facilitate the identification of the communication circuits or channels that suffer from high error rates.

17.4 Communication Network Processors

Communication Network Processors (CNPs) shall be dedicated to data exchange with external computer systems, such as EGAT's EMS and the Authority's future MDMS, and with network access nodes, such as those of local data communication service providers in support of TDMS communications with SCB Interfaces. All CNPs shall be from the same model family, use the same operating system, and use commercially available hardware for their communication channel interfaces. To maintain system security and prevent any unwanted CNP data traffic, firewalls shall be used.

17.5 Backup and Archive Storage

Storage devices shall be used for on-line backup of the TDMS data and software and for archival storage of IS&R data. The Contractor's backup and archive storage solution shall comply with the following minimum requirements:

1) Shall support Storage Array Network (SAN) technology and, as applicable, Network Attached Storage (NAS) technology.

2) Include redundant (fault tolerant) RAID 0, 1, 5, or better technology.

3) In the case of IS&R, have the capacity to retain up to 2 (two) years of stored data. This is in addition to the existing two (2) years of data that shall be migrated from the existing SCADA/EMS/DMS systems.

4) In the case of system backup and archiving, have the capacity for two (2) years of model and configuration data.

5) Have the necessary throughput, capacity, and redundancy to meet overall system performance requirements (refer to Clause 15).

6) Include ports of fiber channel host interfaces where applicable.

7) Include redundant hot-pluggable power supply technology.

8) Include a redundant cooling system.

9) Support local and remote data replication.

10) Support mirrored write-back cache.

11) Support clustered servers.

12) Include controller password protection for configuration control.

13) Include monitoring and controlling units and software with respect to reporting storage health, performance, and utilization statistics.

The TDMS shall also include rewritable single-platter DVD drives for general storage purposes. The DVD drives shall be capable of reading and writing with CD-ROM media. In addition, a management system for such media as tape and DVD shall be provided for the off-line storage of archive data.

17.6 Local and Wide Area Networks

The Contractor shall be responsible for implementing all necessary LANs at each data center and control center. This includes provision of all associated equipment allowing the TDMS at each center to connect with the Authority's Corporate WAN facilities, such as the optical fiber backbone communications system. It also includes all equipment and devices that will be needed to interface the

TDMS with the high-speed data links that the Contractor is responsible for setting up via others to provide TDMS access to the required cellular networks of local service providers.

17.6.1 TDMS LANs

Each data center and control center LAN shall be redundant in configuration and shall be based on 10/100/1000 Mbps Ethernet (IEEE 802.3) technology. The Contractor shall provide all necessary firewalls, routers, network switches, etc. LAN cabling shall be of Category 6 UTP.

Each LAN comprising the redundant LAN shall be implemented with separate hardware, including chassis and power supply. Where modular network hardware is supplied, the circuit boards shall be "hot" swappable, such that it is not necessary to power down the entire chassis to replace a single card. The network design shall provide dedicated bandwidth for each LAN segment (switched technology) and facilitate the addition of future LAN segments.

The malfunction of any piece of equipment connected to a LAN shall not disrupt LAN operations. Similarly, on/off powering or connection/removal of equipment shall not be disruptive.

On-line reconfiguration and enhancement of network hardware and software shall be supported via authentication and password-protected administrative interfaces. The network hardware shall support the Contractor's configuration software management tools.

17.6.2 TDMS WAN

To create the TDMS WAN, the Contractor shall connect the TDMS LANs to the Corporate WAN, i.e., the Authority's optical fiber backbone communications system. This shall include all necessary firewalls, routing switches, and cabling. Communications shall be IP-based.

17.7 Firewalls

17.7.1 General

The Contractor shall provide dedicated and redundant hardware modules for firewalls along with all supporting network equipment including routers and network switches. Where the network design has cascaded firewalls, the Contractor shall utilize firewalls that are from different vendors to maximize security. Moreover, the hardware used for firewalls shall be different depending on the specific type of interface, data traffic, and points of access being monitored and controlled from a TDMS security perspective. For example, the hardware used for the DMZE firewalls shall be different from the hardware used for security monitoring and control of the data traffic between the TDMS and its FDIs, where performance requirements are also critical.

Within this context, centralized security management software is also required. This Contractor software shall control system security related to all network equipment as well as TDMS servers and devices. Supported by log servers, the software shall include log analysis, report generation, and other security related functions as necessary to prevent, detect, and mitigate security attacks.

All firewalls shall support the necessary throughput and redundancy to meet overall system performance requirements. The number of ports provided shall have fifty (50) percent spare for usage by the Authority in the future.

They shall gracefully and automatically re-establish required connections as needed and in compliance with secure connection establishment procedures.

The Contractor shall supply a list detailing the interface ports and services required for full and secure TDMS functionality. This list shall include all information required to define the firewall rules including direction, protocol, interface port number, and associated service for each network connection.

17.7.2 Next Generation Firewalls

The firewalls shall be of next generation type using advanced security and control capabilities at throughput speeds that will allow authenticated users, computers, and applications to access TDMS services with no perceivable delays. In this respect, each Next Generation Firewall (NGFW) shall include the following features:

1) Highly effective security backed by extensive threat intelligence to reduce the risk of a data breach.

2) Integrated Intrusion Prevention System (IPS), Web filtering, IP reputation, antivirus, and advanced threat protection.

3) Deep inspection of network traffic to identify applications, users, devices, and threats through granular policy controls.

4) Single operating system and consolidated user interface for all security and networking capabilities.

5) Centralized “single-pane-of-glass” management and reporting capabilities to visualize the NGFW’s security effectiveness and help determine what strategic security policies to implement, such visibility making it easier to control device configurations, security policies, firmware installations, and content security updates as well as monitor what is happening in the network through logging, in-depth reporting, and event management.

6) Highly reliable core firewall capabilities such as:

    a) *Authentication* – Enforcement of user and application password construction rules such as minimum length, inclusion of non-alphanumeric characters, and maximum validity period.

    b) *Access Control* – Different TDMS access levels for internal and external users (both persons and applications) including none, read only, read/write, and execute. Internal TDMS users shall be denied access to the Internet.

c) *IP Spoofing* – Protection against attacks in which a would-be intruder outside the firewall configures its machine with IP addresses on the internal TDMS LANs.

d) *Prevention of Denial of Service* – Protection against attacks that are characterized by attempts to deny service through overrunning buffers, filling the firewall disk, or overrunning log files, such attacks resulting in rejection of packets where they can be recognized or, where they are not recognized, resulting in shutting down or denying external access when overruns occur rather than continuing to operate with partial capability.

e) *Packet Filtering Restriction* – Based on both source and destination IP addresses.

f) *Stateful Inspection* – Determining which port numbers are used by which connections and, when a connection closes, shutting down access to the port used by the connection until another authorized user establishes a new connection.

g) *Proxy Servers* – Application proxies including HTTP, FTP, UDP, TCP, and others as needed for the relevant TDMS functions, access to these services being customizable based on user ID and IP address.

h) *Network Address Translation (NAT)* – Permitting the Authority to hide the IP addresses used on the internal TDMS LAN from external view.

i) *Notifications* – Recording all break-in attempts in a log file.

17.7.3 Firewall Configuration

The Contractor shall be responsible for the configuration of firewalls with Authority assistance to define the access rules. The Authority expects the following general access rules to be implemented:

1) Remote control of the power system from external points of access shall only be permisable by properly authorized personnel at the TDMS control centers.

2) Access from the TDMS to systems and networks on the Corporate WAN shall be allowed. This shall not include access to the Internet.

3) Access to the TDMS from users and systems on the Corporate WAN shall be limited by IP address and user (or account) name.

4) Corporate users at selected nodes (IP addresses) shall be permitted access to the IS&R function as replicated in the DMZE for read-only purposes. The IS&R access control facilities as installed in the DMZE shall be used to further limit access.

5) Corporate users at selected nodes shall be permitted access to the Web services to be installed in the DMZE.

17.8 Field Device Interface Communications

The TDMS shall communicate with substation FDIs (i.e., SRTUs and CSCSs) over the Authority's optical fiber backbone communications system. To communicate with feeder pole-top FDIs other than SCB Interfaces, the optical fiber backbone communications system augmented by UHF radio cells shall be utilized. In case of SCBs, the TDMS shall communicate with their FDIs via the cellular networks of local service providers.

The TDMS Data Acquisition (DAC) nodes corresponding to FDIs other than SCB FDIs shall include all necessary Contractor-provided hardware and software. This includes FEPs (refer to Clause 17.3) and all associated cables and connectors.

With respect to the SCB Interfaces, the Contractor supplied and installed CNPs (refer to Clause 17.4) shall be equipped with all necessary interface equipment and drivers to establish the required data communication links between the TDMS and these interfaces. The capability to support high-speed data links to as many as four separate cellular networks shall be provided.

17.9 Time and Frequency Support

As noted elsewhere in these Technical Specifications, an Authority time and frequency facility used to determine Universal Coordinated Time (UTC), power system time, time deviation, power system frequency, and power system frequency deviation will be provided at each data center as a common server resource. UTC will be obtained from the satellite constellation comprising the Global Positioning System (GPS). In this respect, it can be assumed that the time receiver will provide an overall accuracy of ±40 ns (±150 ns peak) when tracking satellites and shall include an offset to permit correction to local time.

Thus, the TDMS shall include an internal facility capable of using the output time and date reference signals from the Authority's time and frequency facilty to synchronize, for example, the internal clocks of TDMS servers and processors. Moreover, using Greenwich Mean Time (GMT) and taking communication path delays into account, the TDMS shall use the time and date reference signals to synchronize the internal clocks of Field Device Interfaces.

TDMS time at data centers shall frequently be compared to the time standard unit and synchronized to keep system time within ± 1 (one) millisecond of standard time for use in time tagging of all data, alarms, and events.

A common time code output format such as IRIG-B shall be supported. Also, as a minimum, four (4) communication ports shall be provided with drivers capable of supporting communication protocols such as NTP, SNTP, and TCP/IP.

Upon loss of signal from the Authority's time and frequency facility, the TDMS shall revert to an internal time base. The stability shall be 2×10^{-6} or better with an output time drift not exceeding 30 milliseconds per day. The time shall return to within ±1.5 ms of UTC within five minutes of reacquisition of signal.

The TDMS internal facility shall include an alphanumeric display and keypad on its front panel. The display shall show the time along with the status of the internal facility and the signals from the Authority's time and frequency facility. The internal facility shall also support entry of any relevant setup parameters.

17.10 Remote Workstations

Dispatcher/supervisor and data engineering workstations, as remote clients, shall include all hardware and software necessary to facilitate optimum user communications with the servers comprising the TDMS at each data center. They shall include facilities to detect the loss of input power, execute an orderly shutdown upon loss of input power, and automatically resume operation when power is restored.

As a minimum, they shall consist of the following equipment:

1) Multiple monitors.

2) A tower processor.

3) An alphanumeric keyboard and cursor control device.

4) An audible alarm.

5) For Data Engineering workstations, uninterruptible Power Supply (UPS) units.

Each workstation shall represent the latest available technology with the following pre-installed components:

1) Latest long-term supported Windows or Linux operating system. The installation shall include all latest releases of security patches.

2) Two (2) Gigabit Ethernet NICs (10/100/1000 Mbps).

3) Graphics card that supports multiple displays to the specified resolution of the workstation monitors.

4) 27-inch LED monitors with a resolution of no less than FHD (1920 by 1080 pixels).

5) Wireless keyboard supporting English and Thai.

6) One optical wireless mouse with buttons and scroll-wheel.

7) Built-in loudspeaker for audible alarming and use with future functions.

The monitors shall be supplied with tilt and swivel bases, including a mounting plate for desktop stand. The tilt range shall be from a minimum of 5 degrees downward (measured from a plane perpendicular to the face of the screen) to 30 degrees upward. The monitor base shall have a swivel range of ±30 degrees from a nominal centered position. The monitor support bases shall have a height adjustment

range of 3.5 inches from the lowest to highest position. The monitor bezel shall be a thin-edge design, with a bezel thickness of 20 mm maximum.

Each Data Engineering workstation shall be delivered with a single (non-redundant) UPS that shall operate continuously as a buffer between the normal ac power supply and the workstation's desktop PC. The UPS shall be appropriately designed and rated for the environmental conditions and expected workstation load. Each UPS shall include maintenance-free sealed batteries and have a 50% surplus capacity. The batteries shall be sized to power the desktop PC for a minimum duration of thirty minutes at the maximum ambient air temperature and relative humidity expected following loss of ac power supply and air conditioning equipment.

17.11 Workstation Furniture

As in Clause 6.1 and Exhibit 15-2, consoles and chairs are required as furniture supporting all control room workstation positions. In this respect, the workstation and PC equipment at each dispatcher/supervisor position in the TDMS control rooms shall be installed in ergonomically-designed furniture, suitable for 24-hour, 7days per week service with minimum wear. The furniture shall be provided to include all parts and accessories required for installation and use of the workstation. The essential features of the furniture shall be as follows:

1) Modular low-profile open top design presenting a modern contoured appearance with no exposed fasteners on any surface.

2) Curved to match the ergonomic requirements for reach and visibility.

3) Under counter space for the workstation's processor and the Dispatcher's PC processor (refer to Clause 17.12).

4) Storage modules with file drawers.

5) Separately adjustable height work surface with swing-arm monitor mounts. The work surface and monitor mounts shall move independently to accommodate individual Dispatcher requirements.

6) Adequate space for writing, monitors, telephone, and radio. The writing surface shall be burn and stain resistant and fully integrated as part of the workstation module.

6) Constructed with a metal sub-frame providing structural support for the workstation equipment mounts and the exterior panels that enclose the workstation modules. Each modular sub-frame shall be securely attached to the sub-frames of its adjacent modules to form a rigid workstation unit and a seamless equipment mounting enclosure for the full length of the workstation.

7) Individual workstation modules incorporating height adjusters to compensate for uneven floors and ensure adjacent modules are properly aligned.

8) Sub-frame and mechanical fastening system capable of reconfiguration and additions with no on-site cutting, drilling, or machining required. Each separate module shall be rigid and self-

supporting to permit individual removal, relocation, or modification of adjacent modules. All mounted equipment and subassemblies including all drawers and speaker brackets shall be interchangeable among all modules.

9) Workstation exterior panels attached to the sub-frame by means of concealed hardware and removable without the use of tools. Individual panels shall be hinged, with concealed hinges, to allow convenient installation of, and service access to, internally mounted equipment.

10) Exterior panel colors and finishes selected by the Authority during project implementation.

11) A task lighting system such that the light falls on the work surface only, not in the Dispatcher's eyes, nor in a way as to create glare on any of the workstation's flat monitors.

12) Separate credenzas supplied and installed in addition to the workstations. Providing additional shelf and drawer space, the credenzas shall not exceed the height of the other workstation furniture, all of which shall be designed to present an overall pleasing and functional effect.

13) Workstation chairs including a seat-lifting system that includes levers and jacks. The chairs shall be designed for heavy-duty and comfort and finished with burn and stain resistant materials.

Within the above context, the Contractor's proposal shall have included catalogues showing different furniture models and sizes as possible alternatives for Authority consideration. From these alternatives, however, the Contractor shall have clearly identified the specific set of furniture that constitutes the actual offer. The information shall include all relevant model numbers, configuration and sizing details, and all other information describing unambiguously how the Authority's furniture requirements shall be met. Where a specific alternative to the actual offer is provided, this shall have been identified in a clear and unambiguous manner as well.

17.12 Dispatcher PCs

The Contractor shall provide state of the art desktop (tower) PCs that Dispatchers will use to access the Corporate WAN independently of the TDMS. These PCs shall have no direct connection to the TDMS. Monitors and keyboards shall be mounted on the same furniture used to install the Dispatcher workstations.

The PCs shall represent the latest technology available at the time the Contractor orders them. They shall comply with the following minimum requirements:

1) Monitor: As per Remote Workstation, i.e., 27" LED, FHD (1920 x 1080).

2) Processor: Intel 7th Generation Core^{TM} i7, or equivalent.

3) Memory: 8 GB (expandable).

4) Storage of SSD type: 256 GB.

5) Graphics: NVIDIA, or equivalent (2GB).

6) Display support: DVI/HDMI, DisplayPort.

7) Ports: 3 x USB, 1 x HDMI, 1 x Ethernet, 1 x Serial, headphone/microphone.

8) Network: 10/100/1000 Ethernet.

9) Disk drive: Internal DVD+/-RW.

10) Keyboard: Wireless, both English and Thai.

11) Mouse: Wireless optical.

12) Operating system: As per Remote Workstation, long-term supported Windows or Linux operating system.

13) Software: MS Office (Thai) including licenses.

14) Antivirus software: All latest security patches.

17.13 Network Test Sets

The portable PCs for operating, testing, and maintaining the TDMS and its FDI interfaces, from the perspective of diagnosing communication problems, shall be notebook computers with complete access security. Each Network Test Set (NTS) shall be complete with the same operating system as a TDMS workstation. They shall include protocol analyzer software and network sniffer software. The protocol analyzer software shall support analysis of the ICCP and DNP 3.0 data traffic over the TDMS IP network.

At least two ports shall be used for the network connections, e.g., USB ports along with all necessary external adapters. Two ports are required for proper monitoring of bi-directional master/slave communications. As a minimum, the test sets shall operate at rates up to 57.6 kbps. Otherwise, their capabilities and features shall be like those of the DAC simulators (refer to Clause 17.16).

17.14 Video Display Wall

The video display wall for each designated control room shall consist of Laser-lit rear-projection cubes offering the latest generation of Laser and Digital Light Processing (DLP) technology along with all associated equipment such as the video wall's graphics display server. The cubes shall form a continuous single large display that is 3 monitors high and 3 monitors wide to maintain the current video wall size. The diagonal size of each cube shall be 70". The aspect ratio of each cube shall be 16:9.

17.14.1 Installation

Each of the projection cubes shall include a complete frame and mounting system, the projector and accessories, all required data and video cabling, and all internal power wired to power junction boxes furnished by the Contractor.

The individual projection cubes shall be of rigid modular construction, fabricated to minimum tolerances to ensure accurate and repeatable alignment. The projection cubes shall be capable of multiple assemblies, disassemblies, and re-assemblies to accommodate factory inspection and test, shipping, installation, and possible relocation. The video display wall shall be properly supported and framed to ensure that there is no perceptible jitter to the projected images caused by mechanical vibration of the overall structure.

The display structure shall be directly anchored to the concrete structural flooring of the control room with all projection cubes positioned in the control room wall opening so that their monitors are flush with the wall's front surface. The lowest row of monitors shall be adjusted to a suitable viewing height above the control room's raised floor. This height shall be based on standard ergonomic rules for vertical and horizontal viewing angles in support of the control room's seated Dispatcher positions. The Contractor's ergonomic design and viewing angle calculations shall be subject to Authority review and approval.

The Contractor shall provide and install any additional bracing required to stabilize the display wall. If any non-metallic materials are used as the carrier and/or support structures, the Contractor shall submit a document identifying the chemical composition of the material(s) including fire rating and off-gassing properties.

The front side of the display wall shall include fascia panels to provide a pleasing finished appearance. These panels shall be covered with sound adsorbing material. The Contractor shall also provide and install trim material to bridge any gap between the installed display wall assemblies and the rough opening created to accommodate the display wall. The panel and trim materials shall match the architectural finish and color scheme of the control room. All interior surfaces of the projection units housed in each cube shall have a flat black, non-reflecting finish.

The projection cubes shall be installed, aligned, and edge-matched by the Contractor for cube-to-cube uniformity and continuity, with proper registration and alignment between cubes and without visible changes in color, color temperature, projected image size, contrast, or light intensity from cube to cube. In this respect, adjacent cubes shall be physically separated by no more than 0.2 mm with images across monitors presenting a pixel-to-pixel alignment of less than 0.7 mm.

The Contractor shall adjust the installed projection cubes to provide the optimum vertical and horizontal viewing angles. The projected images shall be clearly visible and legible from all viewing angles within ±80 degrees horizontally and ±35 degrees vertically. Each projection cube shall be capable of motorized remotely controlled 6-axis adjustment such that one technician can mechanically adjust/align each cube's geometry from the front side of the display wall. Similarly, each cube shall be capable of motorized mirror adjustments from the front side of the display wall. The means to lock and unlock all adjustments and alignments shall also be provided.

17.14.2 Graphics Display Server

The Contractor shall supply a multi-monitor graphics display server that shall provide high-resolution display signals to the projection cubes. The display server shall have the capability to display full graphics and standard video images on each display unit at a minimum resolution of Full HD (1980 x

1080 pixels). For all graphics applications, the graphics display server shall treat the entire group of projection cubes as a single display including implanted windowed data, graphic, and/or live video displays.

The graphics display server shall enable Dispatchers to execute TDMS functions via the video display wall, which shall include the ability to execute power system SCADA commands. Hence, within this context, the video display wall shall serve as another workstation monitor.

As a minimum, the server from an overall perspective shall support the following types of input:

1) VGA to FHD (1920 x 1080 at 60Hz)

2) Analog (DSUB 15-pin connector)

3) Digital (DVI-D, HDMI)

4) Video (Composite, S-Video, Component-HD)

The graphics display server shall be integrated with the control room's TDMS LAN via redundant 10/100/1000 Base-T Ethernet (Gigabit Ethernet) interfaces. Communications with the TDMS shall be supported using the TCP/IP protocol. The server shall be configured with dual power supplies and dual network interface ports that shall provide for automatic failover of the network interface in the event of a network or port failure.

The server shall obtain graphics information to be shown on the video wall from the control room's TDMS workstations. Authorized users shall have the capability of positioning a window of any size and aspect ratio anywhere within the video wall, including across projection display unit boundaries. The graphic server shall support the presentation of any workstation display, including text, help, and tabular displays.

In addition, the server shall be able to display simultaneously up to four standard (PAL) video signals as a minimum. These video signals will be available from outside broadcast or cable sources, and will be provided as composite video signals. The server shall be able to display the video sources as multiple separate windows anywhere within the video wall. Moreover, the server shall be able to display live images from the Authority's CCTV system that will be deployed for the security monitoring of Authority substations. Such displays shall be capable of being requested by the Dispatcher when substation security alerts from the CCTV system are received and reported by the TDMS. These alerts shall be treated by SCADA in the same way as power system network alarms (also refer to Clause 16.4).

The server shall also support input signals from mobile devices such as smart phones, tablets, and laptop PCs via wireless communications. Such support shall be subject to appropriate security features such as user authentication. Within this context, video wall display (as in "screen mirroring") shall be limited to display of mobile device content only, i.e., no power system control or execution of any other TDMS function shall be possible from such devices.

The graphics display server shall be controlled through a secure user interface that allows authorized users to control all capabilities of the server through a network application, including as a minimum:

1) Opening and closing TDMS application displays from any Dispatcher workstation.

2) Defining, editing, and saving display configurations.

3) Performing remote diagnostics on the server.

4) Controlling the projectors such as on, off, standby, brightness, and contrast.

The user interface shall be Windows based and available through the LAN. It shall have an automatic display configuration feature that can open, close, or adjust the size of multiple windows at pre-determined locations at a specified time of day or day of the week, with no user intervention. The server shall include wireless keyboard and mouse ports that shall provide all control and configuration features for the projected display as described above.

The Contractor shall provide the interconnection cables between the server and the projectors. The server interface equipment shall be strategically located to minimize cabling.

The server's output to each projection display unit shall be through a direct digital link conforming to the latest version of the DVI (Digital Visual Interface) standard. The server shall be a standard rack-mount assembly, mounted and secured to the display unit structure with theft-proof mounting on a pullout tray by the Contractor. The server shall be installed within the projection cube base modules and shall be front accessible.

When the graphics display server receives a command to show a new display or windowed display via one of the projection cubes, the new display format shall be generated completely within one (1) second, without any interference or delay to one-second periodic updates to all other projection cubes handled by the server, regardless of the current configuration of display windows on the other projection cubes.

The application updates coming from the SCADA servers of the TDMS shall be displayed on the video display wall without delay at the same speeds with which they are displayed on the TDMS workstations connected to the same network, such speeds being a function of the TDMS. The capability of the video display wall to support this feature shall be demonstrated during TDMS factory testing.

17.14.3 Video Wall Maintenance

The video wall design shall permit maintenance personnel to easily perform diagnostic tests as well as adjust each projection display unit. This shall include easy access to all display components for cleaning, adjustment, replacement, and other maintenance tasks.

All projectors shall be mounted with an identical fixed geometric relationship to the mirror and monitor and capable of being removed, repaired, and reinstalled in any display unit with minimal readjustment.

17.14.4 Projection Cube Characteristics

Each projection cube shall consist of a data/graphics projector, optical quality mirror(s), a high contrast rear-projection monitor, and signal interface modules contained in a modular light-tight cabinet. The projector and mirror mounts shall be adjustable for precise alignment of the projected image. All projection units shall be identical, and shall be designed to interlock together to form a rigid display wall when assembled in a multiple monitor array.

The data/graphics projectors shall be high-resolution single-chip DLP projectors meeting or exceeding the following criteria:

1) Minimum native resolution of 1920 x 1080 pixels.

2) Minimum on-screen brightness of 500 cd/m^2.

3) Brightness uniformity greater than 95%.

4) 16.7 million colors.

5) Illumination system life of at least 100,000 hours in continuous 24-hour, 7 days per week operation.

6) Illumination system shall use redundant RGB Laser diode for illumination of RGB colors without use of any color wheels.

7) Motorised adjustments in xy plane and provision for focus and zoom.

8) Minimum on-screen contrast ratio of 1800 to 1.

9) Mean Time Between Failure (MTBF) greater than 150,000 hours in continuous 24-hour, 7 days per week operation.

10) Configurable for remote and redundant power supply.

The data/graphics system shall have a continuous duty cycle of 24/7 for color calibration and brightness uniformity using automated software and shall support a manual (on-demand) feature override function.

The display unit monitors shall be wide-angle, high-contrast, multi-element, cast acrylic, rear-projection monitors specifically designed for use with high brightness single lens projectors. The viewing side of the monitors shall have an abrasion resistant, anti-glare surface. On-axis gain shall be 1.0 minimum with a minimum horizontal and vertical ½-gain angle of $\pm$ 36 and $\pm$ 33 degrees respectively.

17.15 Printers

17.15.1 Multifunction Printers

The technology, capabilities, and features of the multifunction printers to be supplied and connected to control center LANs by the Contractor shall be based on the following minimum requirements:

1) Functions: Print, copy, scan, fax.

2) Print technology: Laser.

3) Print speed: More than 20 pages per minute in black and color.

4) Duplex printing: Automatic

5) Resolution: 600 x 600 dpi (black and color).

6) Duty cycle: 15,000 pages per month.

7) Print languages: Postscript, PDF, etc.

8) Paper sizes: A4, A3, letter, legal.

9) Paper trays: Input/output capacity of 250 pages.

10) Connectivity: USB, Ethernet, RJ-11.

11) Memory: 256 MB.

17.15.2 Black and White Printers

The technology, capabilities, and features of the black and white printers to be supplied and connected to control center LANs by the Contractor shall be based on the following minimum requirements:

1) Function: Print.

2) Print technology: Laser.

3) Print speed: More than 50 pages per minute.

4) Duplex printing: Automatic

5) Resolution: 600 x 600 dpi.

6) Duty cycle: 50,000 pages per month.

7) Print languages: Postscript, PDF, etc.

8) Paper sizes: A4 and A3.

9) Paper trays: Input/output capacity of 500 pages.

10) Connectivity: USB, Ethernet, RJ-11.

11) Memory: 256 MB.

17.16 Data Acquisition Simulators

In addition to the hardware and software supporting the TDMS architecture, the Contractor shall provide portable Data Acquisition (DAC) simulators to be used as field device interface test sets.

These simulators, in essence, shall provide the same SCADA functionality as the TDMS so that, by connecting locally to the communication ports of an individual field device interface (i.e., at the site where the interface is located), they can be used to verify that the field device interface data and control points are properly mapped from a TDMS database perspective and, in this respect, can be exercised and shown to be fully operational as though they were being exercised from the TDMS itself.

The DAC simulators shall include the field device interface diagnostic capabilities of the TDMS. To communicate with a field device interface, they shall support secure DNP 3.0 over IP.

Each DAC simulator shall include multiple communication ports and all necessary interface connectors and cables to allow direct on-site connection of the simulator to the communication ports to be provided with each type of field device interface (one for normal TDMS operations, the other for field device interface diagnostics).

The DAC simulator platform shall be a PC representing the latest notebook technology available. The key board shall accommodate Thai as well as English characters. Otherwise, its capabilities and features shall be specifically selected to ensure that it is entirely suited to its intended use. It shall be delivered with a case sufficiently sized to contain and safely protect all components. Both the notebook PC and case shall be sufficiently rugged to withstand frequent transportation and use under typical field conditions. Each notebook PC shall comply with the following minimum requirements:

1) Monitor: 15” LED, FHD (1920 x 1080).

2) Processor: Intel 7th Generation Core^{TM} i7, or equivalent.

3) Memory: 8 GB (expandable).

4) Storage of SSD type: 500 GB.

5) Graphics: NVIDIA, or equivalent (2GB).

6) Display support: DVI/HDMI, DisplayPort.

7) I/O Ports: 3 x USB, 1 x HDMI, 1 x Ethernet, 1 x Serial.

8) Network: 10/100/1000 Ethernet, Wi-Fi (IEEE 802.11).

9) Slots: SD card reader (64GB).

10) Disk drive: Internal DVD+/-RW.

11) Keyboard: Wireless, both English and Thai.

12) Mouse: Optical wireless type.

13) Battery: Li-Ion type (60Wh).

14) Operating system: Latest long-term supported Windows or Linux operating system.

15) Antivirus software: All latest security patches.

17.17 Spare Parts

The Contractor's proposal shall have included a recommended list of spare parts for maintenance and repair of the equipment to be delivered as part of the TDMS scope of supply. The recommended list shall be sufficient to cover a two-year period corresponding to the total quantity of TDMS equipment to be delivered. The availability of these parts shall be guaranteed for a period of no less than ten (10) years from the date of the latest delivery of the TDMS equipment or assemblies containing these parts. The Contractor shall commit to notifying the Authority at least six (6) months in advance of any part or assembly becoming unavailable for purchase.

17.18 Special Tools and Accessories

In addition to the specified TDMS hardware, the Contractor shall supply any special tools and accessories, including peripheral devices or equipment that may be required for the installation, testing, commissioning, proper operation, and maintenance of the TDMS. This shall also include all relevant software tools and utilities.

17.19 Operating and Construction Requirements

All TDMS equipment shall operate and be constructed in accordance with the following requirements.

17.19.1 Environment

The TDMS equipment shall be able to operate over an ambient temperature range of 10 to 38 °C, with a maximum rate of change of 8 °C per hour, and over a relative humidity range of 30 to 95% non-condensing.

17.19.2 Equipment Noise

The noise generated by the equipment in any enclosure, including desktop equipment, shall not exceed 50 dbA beyond 1 meter from the enclosure. Sound-deadening enclosures shall be provided where necessary to meet these requirements.

17.19.3 Enclosures

Except for workstations, monitors, keyboards, cursor positioning devices, printers, and processor terminals, all equipment shall be mounted in enclosures. These enclosures will be provided by the Authority as part of the data center facilities. Typical design features are as follows:

1) 19" racks behind plexiglass doors.

2) Floor-mounted with front and rear access to hardware and wiring.

3) Enclosure height not exceeding 2000 mm (80 inches).

4) Moving assemblies within the enclosure such as swing frames or extension slides.

5) Cable entry through enclosure top or bottom.

6) Cooling air drawn from data center air-conditioning facilities.

Equipment installations in the Authority-provided enclosues shall meet with the following requirements:

1) Wiring shall be neatly arranged and securely fastened to the enclosure by non-conductive fasteners.

2) Wiring between all stationary and moveable components, such as wiring across hinges or to components mounted on extension slides, shall allow for full movement of the component without binding or chafing of the wire.

3) All materials used in the enclosures including cable insulation or sheathing, wire troughs, terminal blocks, and enclosure trim shall be made of flame retardant material and shall not produce toxic gasses under fire conditions.

4) All cables passing under a raised floor shall be neatly arranged in wire troughs and rated as NEC Class 2 Plenum cable. Cables shall be tested to NFPA 262-1985 Test for Fire and Smoke Characteristics of Wires and Cables to a maximum peak optical density of 0.5, a maximum average optical density of 0.15, and a maximum allowable flame travel distance of five feet.

5) All wire and cable connectors and terminators shall be permanently labeled for identification. All connection points for external cables and wires shall be easily accessible for connection and disconnection and shall be permanently labeled.

6) Wherever operating voltages in the hardware exceed 50 volts, the hardware shall be covered or shielded from accidental contact and shall be labeled accordingly.

17.19.4 Assembly and Component Identification

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. Changes to assemblies shall be indicated by an unambiguous change to the marked revision level. All printed circuit card cages and all slots within the cages shall be clearly labeled. Printed circuit cards shall be keyed for proper insertion orientation.

17.19.5 Enclosure Grounding

A safety ground in accordance with Thai codes shall be provided within each enclosure and shall connect to the ground (green) wire of the ac power input. Enclosure grounding shall be subject to the Authority's approval.

17.19.6 Interconnections

The Contractor shall supply all cabling between component units of the TDMS within each facility. Plug-type connectors with captive fasteners shall be used for all signal interconnections. The connectors shall be polarized to prevent improper assembly. Each end of each interconnection cable shall be marked with the cable number and the identifying number and location of each of the cable's terminations; this information shall agree with the drawings. Each cable shall be continuous between components; no intermediate splices or connectors shall be used. Terminations shall be entirely within the enclosures.

17.19.7 Space Description

All computer, communication, and control rooms will have raised floors with removable panels. Dimensioned plan views of the data and control center rooms will be provided during project implementation. They will be used to finalize placement of the TDMS equipment.

17.19.8 Power Distribution and Protection

The Contractor shall provide all power cabling and connection hardware that is necessary to distribute electrical power to the Contractor supplied TDMS equipment from Authority available power sources. In this respect, the TDMS equipment shall be powered from diverse power sources such that the loss of any one of them shall not result in the loss of any critical TDMS function.

In distributing power within enclosures, workstations, peripherals, and other components of the TDMS, the Contractor shall supply and install all fusing, circuit breakers, switches, and surge devices necessary to protect the TDMS hardware. Each enclosure's single input power circuit, for example, shall include a circuit breaker typed and sized in accordance with the Contractor's recommendation. Power connections between the enclosures and the input cable shall be dead-front connectors located within the enclosures.

18. SCADA Functions

The TDMS requirements that concern SCADA related functions such as Data Acquisition, Data Exchange, Data Processing, Supervisory Control, Load Shedding and Restoration, and Switching Order Management are presented in this clause. Relevant capacity and performance requirements for these functions are presented in Clause 15.

18.1 Data Acquisition

The TDMS shall collect real-time telemetered data from the following data sources:

1) ***Field device interfaces at substation sites*** - These are the Substation Remote Terminal Units (SRTUs) and Computer-based Substation Control System (CSCS) Interfaces.

2) ***Field device interfaces outside substations*** - These are the Feeder Remote Terminal Units (FRTUs) and Feeder Device Control Units (FDCUs), otherwise referred to as FDIs, located at pole-top sites and used to interface with Remote Controlled Switches (RCSs), Line Reclosers (LRCs), Line Recloser/Regulators (LRRs), and Switched Capacitor Banks (SCBs).

A data source may collect data from more than one location or a location may have more than one data source. In any event, the TDMS shall always associate telemetered data with the location rather than the data source, so that the identity of all data presented to TDMS users shall include the location name rather than the source name. Where applicable, data presentation shall also be organized by location rather than source name. The Authority will determine the mapping of the location name to the data source.

In addition to telemetered data, the TDMS shall support the following types of data:

1) Non-telemetered data entered by the user.

2) Calculated data generated by the data processing function.

3) Calculated data generated by applications.

This data may be of any type specified in Clause 18.3 unless explicitly stated otherwise, all requirements in this and other clauses 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.

18.1.1 Data Acquisition Protocols

To acquire telemetered data from its field device interfaces, the TDMS shall support DNP 3.0 and the latest secure version of DNP over IP. In this respect, data acquisition shall utilize the following DNP 3.0 defined modes of operation:

1) Class 0, 1, 2, and/or 3 polls by the TDMS. This shall include:

    a) Integrity and report by exception polling.

    b) Sending selected status or analog points on demand.

2) Unsolicited (spontaneous) Class 1, 2, and/or 3 responses by FDIs due to a power system event. This shall include sending an analog or status point value in the event:

    a) An analog value exceeds an individually configurable deadband around its previously reported value.

    b) An analog value exceeds an individually configurable threshold.

c) A status point changes state.

18.1.2 Acquisition via Polling

In data acquisition via polling, the TDMS shall initiate data collection by transmitting a periodic scan request to the data sources. The scan start-time shall establish the time after the start of an hour that the first scan of the data source or group of data sources is to occur. The scan periodicity shall be set between 1 second and 3600 seconds to a resolution of one second. The TDMS shall support parallel (concurrent) scanning of sources on multiple IP-based communication circuits. This shall include the capability to poll data sources that share a communications circuit.

18.1.3 Spontaneous Reporting

Unsolicited data acquisition shall be spontaneously initiated by data sources, typically when changes in source input data from field devices are detected or when processes within the data source determine that data should be reported (for example, periodically). The TDMS 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.

18.1.4 Demand, Programmatic, and Integrity Scans

In addition to normal periodic and spontaneous data acquisition, the TDMS shall acquire data from sources under the following conditions:

1) When requested by a user.

2) When initiated by an application.

3) Periodically in the form of an “integrity” scan. The periodicity of the integrity scan shall be user-adjustable.

Each initiation of a demand, programmatic, or integrity scan shall include parameters to specify the data source to be scanned.

18.1.5 Full Report and Report by Exception

The TDMS shall accept data reported in full and by exception where:

1) Data reported in full concerns the collection of all data source values whether the values have changed or not. In this case, the TDMS shall be provided with the means to process only those values that have changed significantly by applying Authority-adjustable threshold or deadband values.

2) Data reported by exception concerns the collection of data source values only if they have changed, e.g., a status point changes from close to open or an analog value changes and exceeds a deadband. In this case, the TDMS shall store a dead-band value for each value to be reported by exception. This deadband shall be adjustable by TDMS users and shall be

downloaded to the data source upon change of the deadband and whenever the data source is brought on-line.

18.1.6 Enabling and Suspending Data Acquisition

In suspending data acquisition, users shall be able to "remove from scan" any individual point or entire data source. Suspended points and data sources reporting spontaneously shall not be processed nor stored in the database. Suspended points acquired by polling may continue to be polled from the data source, but shall not be processed nor stored in the database. When suspended, polled data sources shall not be polled. Suspended points shall hold their last value unless manually overridden.

The TDMS shall set an "acquisition suspended" quality code for all suspended points and shall make an entry for the points on the off-scan summary (Clause 16.7.12.4). The acquisition suspended quality code shall be distinct from the "telemetry failure" quality code (refer to Clause 18.1.7). When the user enables ("restores") the point or data source, the TDMS shall resume polling or processing the data (as in spontaneous reporting) and updating the TDMS database accordingly. When enabled, the acquisition suspended quality code shall be removed from the affected points, and the affected points shall be removed from the off-scan summary.

18.1.7 Telemetry Failure and Manual Substitution

"Telemetry failure" is defined as any of the following conditions:

1) The inability of the TDMS to complete data collection within a timeout period that can be set between 1 and 60 seconds to a resolution of 1 second.

2) The inability of the TDMS to complete data collection from a data source prior to the next scan of this data source.

3) The inability of the TDMS to complete data collection due to errors in the communications with the data source.

Failed scans with periodicities longer than a threshold (initially 10 seconds) shall be immediately retried (without waiting for the next periodic scan time) and a corresponding "retry count" shall be incremented. Failed scans with scan periodicities less than or equal to the threshold shall not be retried, but the retry count shall be incremented; the scan will be effectively "retried" at the next periodically scheduled scan time. Retry counts shall be reset whenever associated acquisitions prove successful.

When the retry count exceeds a retry limit for a data source, telemetry failure shall be declared, and subsequent scheduled scans shall occur as if the failed telemetry scan had been successful.

If a new transmission is received from a spontaneously reporting data source before the previous transmission has been processed and acknowledged, the TDMS shall attempt to process the incoming data. If the source continues to report data at a rate faster than the TDMS can process the data ("data overrun"), the TDMS shall declare a telemetry failure for this source. The TDMS shall remove the telemetry failure condition after a time specified for all spontaneously reporting sources (initially 30

minutes). The user shall be able to inhibit this failure restoration procedure (for all sources, not individually).

Upon declaring telemetry failure, the TDMS shall set a “telemetry failure” quality code for all affected points and shall make an entry for the points on the off-scan summary. The TDMS shall generate an alarm when a telemetry failure occurs. The alarm shall describe the data source, but shall not list the individual points of the data source.

The last good value of a point in telemetry failure (the value stored in the database immediately prior to the detection of the telemetry failure) shall be retained in the database. For selected accumulator points as described in Clause 18.3.4.4, the TDMS shall automatically substitute another value for accumulator points experiencing telemetry failure.

The TDMS shall support user entry of a substitute value for any point experiencing telemetry failure or for which scanning has been suspended. The TDMS shall set a “manual substitution” quality code for a manually substituted point. When data acquisition is enabled and the point is next successfully (without error) acquired and processed, the value shall be overwritten and the manually substituted quality code shall be reset.

The TDMS shall support user reset of the telemetry failure condition. This shall cause the accumulated retry count to be reset. Otherwise, after telemetry failure reset, the collection of data shall continue, at the normal periodicity, and the transmissions from spontaneous reporting sources shall be processed as normal.

18.1.8 Sequence-of-Events Collection

Sequence-of-events (SOE) data shall be collected from appropriately configured data sources. In addition, whereas traditional SOE data consists of time-stamped reports of status changes, SOE shall be extended to include Authority defined analog points as well. The data source time stamps for both status and analog changes will be to a millisecond resolution.

The data sources will report the availability of SOE data by exception, typically by setting a flag in the header of a reply to a scan request. When the TDMS detects the availability of SOE data, it shall issue a scan request to collect this SOE data.

Collection of the SOE data shall take place at a lower priority than other data acquisition activity or supervisory control action. However, 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. The SOE buffer overflow condition shall be annunciated as an alarm.

Where the data source hardware supports time synchronization, the TDMS shall perform the time synchronization process at a periodicity set by the Authority (initially 15 minutes).

The TDMS shall save the collected SOE data in chronological order as an identifiable separate data set and provide convenient tools and displays by which an engineer can subsequently review recent or past SOE data sets on an individual data source basis. To help analyze events affecting more than one

substation, this shall include the capability to view more than one data set at a time, such as SOE data generated by two or more data sources as the result of a common power system event. The tools for viewing and analyzing SOE data shall have been described in the Contractor's proposal.

18.1.9 Data Acquisition Security

Selected data acquisition communications errors shall be reported to a TDMS security logging system (refer to Clause 11.9). These errors include, but are not limited to:

1) Unexpected replies, including incorrect replies to commands from the TDMS, spontaneous reports from sources not configured as spontaneously reporting, and spontaneous reports from spontaneously reporting sources that have been inhibited.

2) Detection of control commands, scan requests, or other commands not initiated from authorized systems.

3) Replies of incorrect length. The TDMS shall reject over-length replies. This feature shall be specifically demonstrated during factory testing.

4) Communication errors, such as invalid checksum or protocol violations.

In addition to their normal SCADA-related function, the data acquisition front-end processors shall serve as "firewalls" or shall be supported by separate firewalls to protect the TDMS main platform from unauthorized and inappropriate communication attempts from the field device interfaces.

Provision shall be given to record all communications traffic, selectable on a communication circuit basis, to detect unauthorized activity, unusual activity, and attempts to defeat the security capabilities of the TDMS or its electronic security perimeter.

The Contractor's proposal shall have identified and described any security enhancements, such as encryption or additional authentication that may be available to enhance the integrity of the telemetered data.

18.2 TASE.2 Implementation

Where applicable, the TDMS shall exchange data with other computer systems (such as EGAT's EMS and the Authority's OMS) using the Telecontrol Application Service Element (TASE.2) protocol, also known as the Inter-Control Center Communications Protocol (ICCP). In this respect, the TDMS shall be fully compliant with the latest IEC 60870-6-503 and IEC 60870-6-802 standards and, as a minimum, support conformance Blocks 1 and 2 (and 4 if necessary).

The TASE.2 protocol over IP shall be provided. In addition, the capability to implement "Secure ICCP" shall be supported, where Secure Sockets Layer/Transport Layer Security (SSL/TSL) authentication is used, with or without SSL/TLS encryption, and where authentication and encryption is based on X.509 certificates.

Documentation concerning the Authority's current use of TASE.2 will be made available to the Contractor. The Authority, however, will not accept responsibility for errors or omissions in this documentation.

18.2.1 Blocks 1 and 2, SCADA Data

Conformance Blocks 1 and 2 shall be employed for the acquisition of telemetered data from selected computer systems and for the transmission of telemetered data to the same computer systems. The TASE.2 client shall support the following optional client operations:

1) *Data Value object*: Get Data Value, Get Data Value Name, and Get Data Value Type.

2) *Data Set object*: All Client operations. The Critical Data parameter shall be supported.

3) *Data Set Transfer set*: All Client operations.

The Contractor shall provide an interface to TASE.2 for storing and retrieving SCADA data exchanged with other systems. This interface shall be integrated with the SCADA database and the appropriate applications. The SCADA data received via TASE.2 shall be processed by the Data Processing function to apply most of the same processing that would be provided if the SCADA data had been received from a field device interface, except that analogs already in engineering units do not need to be converted from raw counts. TASE.2 shall also support the ability to specify both sign change and additive offsets on a point basis.

For each requested transfer, the user shall be able to set the update rates and define a "Grace Period" for Block 1 data sets. If a report is not received within the given grace period after it is expected, the corresponding points in the database shall be marked as "Not Updated." Whereas, a System Alert message shall be generated to clearly identify the report that was not received, alarms shall not be generated for each of the corresponding points marked as "Not Updated." For Block 2 data sets, the user shall be able to define transmission triggers, define the mode of transmission ("report all" or "report by exception"), and define the integrity scan parameters for report by exception data ("on" or "off", and the time interval between integrity scans).

Telemetered data transmitted to other systems shall be the current value retrieved from the TDMS database. There shall be no restrictions on the selection of any data for transmission. The Contractor shall support all the data quality codes in the TASE.2 protocol by mapping them to the appropriate data quality codes in the TDMS. Also, refer to Clause 18.3.1.

18.2.2 Block 4, Information Messages

Where necessary, and only if an alternative is not available, the TDMS shall use conformance Block 4 to support the bi-directional exchange of information messages between the TDMS and other computer systems such as user-entered text messages or system alerts in the form of text messages generated by TDMS functions, in which case a suitable TASE.2 interface with the TDMS database and its applications shall be implemented.

18.2.3 Access Control

The Contractor shall provide full access control functionality as described in the latest TASE.2 Specification. In this respect, "Bilateral Tables" shall be utilized, where a Bilateral Table represents the agreement between two control centers to identify the data elements and objects that can be accessed via the TASE.2 link and the level of access permitted. Once the link is established, the contents of the Bilateral Tables in the server and client shall provide complete control over what is accessible to each control center. Thus, the server and client tables shall have matching entries for the data and objects to be accessed. Such Bilateral Table requirements are described in Clause 18.2.5.

18.2.4 Alarm and Event Monitoring

The TASE.2 function shall continuously monitor the status of connections on the TASE.2 system and generate alarms or events whenever the status of a connection changes. The alarm message shall clearly state the reasons for a loss of connection. The TASE.2 function shall send all messages to the Alarm and Event Processing subsystem in the TDMS for processing, user notification, logging, historical storage, and archiving. The processing of TASE.2 alarms and events shall follow the requirements specified in Clause 16.4.

18.2.5 Bilateral Table

The TDMS shall implement a Bilateral Table structure (or the functional equivalent) with the required access controls. Since access controls may be different for different clients, multiple Bilateral Tables (one per communicating partner) are required. The Bilateral Table shall be stored in the database and maintained by the database editor described in Clause 9.4. Each object available to each remote client shall be stored including access rights to the object. No object may be served that is not in the database.

18.2.5.1 Contents

All data objects available for exchange shall be listed in a Bilateral Table. No data object shall be served unless it appears in a Bilateral Table. Each data object named in a Bilateral Agreement shall have a corresponding entry in a Bilateral Table. The TASE.2 Specification includes models for Access Control Specification, List of Access Control Specification, and List of Permitted Access. There shall be exactly one Access Control Specification for each TASE.2 client (i.e., other control center) that may have one or more associations with the server. For each client, there shall be a List of Permitted Access for every TASE.2 object in the server's Virtual Control Center (VCC). As part of the VCC's representation of the communication and data management needs of the client, this indicates whether the object is visible to the client and which services the client may perform on the object.

18.2.5.2 Functionality

No data item shall be served to any client unless it appears in a Bilateral Table. It shall be possible to specify different access privileges for the same data object for different clients. For example, for a named data object, it shall be possible to grant read access to Client A, read and write access to Client B, and no access to Client C.

18.2.6 TASE.2 User Interface Requirements

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. Displays shall also be provided to enable the Dispatcher to view the availability of TASE.2 systems and the status of each TASE.2 connection. The user shall be able to access the TASE.2 system remotely, with required access security controls, for problem determination and resolution.

18.2.6.1 Bilateral Table Creation and Editing

A user interface shall be supplied to facilitate entry and modification of the Bilateral Table data. 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.

It shall be possible to create or edit a Bilateral Table while the system is on-line and operating. It shall be possible to create a Bilateral Table by making a copy of existing data. 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. The Authority prefers that the information used to model the Bilateral Table be maintained in a RDBMS. TASE.2 database configuration (Data Engineering) shall be done using the RDBMS. Consistency checks and data type validation shall be performed. After the changes are completed and approved in the RDBMS, they may then be brought on line.

18.2.6.2 Data Set Creation and Editing

The TDMS shall include displays facilitating the creation and editing of data sets. 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.

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. The capability shall be provided via point–and-click to select desired data objects and to create data sets for Block 1 data without having to manually enter the selected point information. 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.

Messages that automatically and dynamically define data sets shall be sent when transfers are started. This ensures that the remote systems definition of the data set matches the local definition. TASE.2 shall also support incoming Dataset Creation and Deletion requests and shall dynamically create server datasets as necessary. 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.

TASE.2 shall support collection of a data item under one Object ID and sending the same data item under another Object ID.

Data set creation shall validate all model changes (data items and connections) before TASE.2 model deployment.

Data set creation shall support creating partial data sets. This feature shall allow the Authority to create a partial data set when one or more items are missing or not granted access by the other end of a connection.

Users may be periodically asked to verify information that is being supplied via TASE.2. Thus, a display facility showing the actual Authority data available to each external entity is required to check the functionality of the process.

18.2.6.3 Connection and Association Control

The TDMS 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). TASE.2 functionality shall include the following display features:

1) An overview display shall be provided that shows the roles and availability of primary and backup TASE.2 systems. This display shall include pages to show the roles and availability 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 TASE.2 system status (e.g., primary, backup) and availability (e.g., available, off-line). Both the status of TDMS systems and other remote computer systems that are active shall be shown.

2) An overview display shall be provided that shows the status of each connection (e.g., active, available, off-line, or error). On a connection basis, controls shall be provided for: separate bilateral agreement, bilateral agreement number, and retry connection rate. The user shall be able to control permissions on a point-by-point basis (both for Domain and VMD data) per connection. 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. The connection status shall include the status of TDMS systems and other computer systems at the remote end. The connection status shall also be available for alarming.

3) Displays that allow the dispatcher or other user to view and control configured Associations shall be provided. Color shall be used to distinguish active and inactive Associations. This display shall show a list of the TASE.2 systems and connections for user selection. The display shall provide the capability of the user to disable Associations. Disabling Associations implies a graceful close of any existing Associations. Entry capability shall be provided for the user to enter the In-service or Out-of-service status tag for each Association or possible Association. For example, TASE.2 systems in alternative control centers will be placed out-of-service until needed. TASE.2 shall dynamically control each Association based on the user-entered in or out of service tag.

The Authority will work with the Contractor to design the dispatcher interface graphical displays and shall have approval rights for all TASE.2 displays provided.

18.2.6.4 Maintenance Tools

The TASE.2 system shall provide tools to allow the user to view and maintain the TASE.2 system and database. These tools shall allow the user to select a data set, connection, or association (or all) to view and modify the selection. The maintenance tools shall provide the following features:

1) Display parameters of data set objects (created by both sides of a connection) including: descriptions, triggers, transmit, and time of creation. 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.

2) Display each data point value, sign, time tagged (time last received), last time of change, and quality code (TASE.2 quality codes). 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.

3) Display all data items by data set (Block 1 and 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).

4) Display all data items Source and Source Object ID along with the Authority Object IDs.

5) Provide an interface to the MMS-EASE debug facility, which can be activated or deactivated on user command. The MMS-EASE debug tool shall provide the user with tools to help solve TASE.2 problems.

6) Provide tools to perform OSI and IP pinging of any connection.

18.2.6.5 Performance Monitoring

The TASE.2 Quality of Service (QOS) attribute shall provide the user with performance statistics on a connection and association basis. Performance statistics shall include: throughput, residual error rate, priority, transit delay, and protection. 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.

18.3 Data Processing

TDMS data processing shall support the following types of data:

1) Data quality

2) Analog data

3) Equipment status data

4) Accumulator data

5) SOE data

6) Non-telemetered data

7) Calculated data

8) Not-commissioned data

9) Redundant data

10) Network status data.

11) Feeder fault statistics.

18.3.1 Data Quality

Quality codes are attributes of database points that identify some conditions affecting a database point. All 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 TDMS functions. Typically, only the most severe code will be presented on a display or report. However, it shall be possible to access and present the most severe code and all codes individually.

For calculated data, the presence of a quality code on any of its arguments shall not disrupt the calculation using that value. The quality code of the calculated value shall be the most severe quality code of the arguments. 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. Results of calculations that are manually suspended by users shall be denoted with a quality code that can be differentiated from the propagation of an "acquisition suspended" or "calculation suspended" quality code from any its arguments.

Quality codes included with data from data sources using standard protocols such as DNP 3.0 and TASE.2 shall be mapped to the TDMS quality codes. Similarly, data transmitted from the TDMS to other computer systems using the TASE.2 protocol shall map TDMS quality codes to TASE.2 quality codes.

Mapping and quality code level-of-severity details shall be finalized during project implementation and shall be based on current Authority practice associated with the existing TDMS; relevant Authority documentation will be provided. The TDMS shall provide the ability of the Authority to change the mapping and quality code severities.

Quality codes shall be accessible from the database as another data item. Quality codes shall be available for use in calculated values as Boolean (true/false) values. For example, a calculated point may be defined for which the value of the result is dependent on the presence of selected quality codes using the conditional execution operators (if-then-else) of the generalized calculations.

It is assumed that each quality code can be set or reset independently of all other codes. Thus, the number of possible combinations of quality codes for a given point shall be 2^n, where n is the number of codes (attributes).

The following quality codes, when applied to a point, shall be interpreted as invalid or "bad" data:

1) Acquisition suspended

2) Calculation suspended

3) Telemetry or calculation failure

4) Field device interface analog-to-digital converter (ADC) inaccuracy

5) Reasonability violation

6) Inconsistent result

7) Long value (for the first accumulator reading after telemetry failure)

8) Data not commissioned.

Values with a manually substituted quality code shall be considered valid.

18.3.2 Analog Data

Prior to storage in the TDMS database, analog data shall be processed to include:

1) ADC accuracy monitoring

2) Conversion to engineering units

3) Reasonability checking

4) Limit checking

5) Rate-of-change checking.

18.3.2.1 ADC Accuracy Monitoring

Certain data sources such as SRTUs will report one or two reference points for each analog-to-digital 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. These limits may be the same limits used for the limit checking function described in Clause 18.3.2.4. When the value of any reference exceeds its high or low limit, an ADC inaccuracy condition shall be declared. All analog points converted by that ADC shall be marked with an "ADC inaccuracy" quality code, the analog points shall be processed as for a telemetry failure, and an alarm shall be generated for the ADC (not for the individual analog points). When the ADC reference returns to within its limits, the quality codes shall be removed, the analog points shall be returned to normal processing, and a return-to-normal alarm shall be generated for the ADC.

18.3.2.2 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*

where the coefficients *a* and *b* define the conversion's scaling and offset factors. The coefficients may be of either sign and shall be individually defined for each analog point.

The following algorithm shall be used to convert selected analog points that use "expanded scale" transducers (this conversion form is also referred to as "clamp to zero"):

If (Telemetered_value ≥ z)

*Converted_value = (a*Telemetered_value) + b*

else Convered_value = 0

where *a* and *b* are as above, and *z* is a positive value defining the lower limit of the transducer.

Analog points representing the tap positions of tap-changing transformers shall be converted into and displayed as discrete integer values.

18.3.2.3 Reasonability Checking

All analog points shall be compared against high and low reasonability limits each time they are processed. The reasonability limits shall represent the extremes of valid measurements for the point's value. An alarm shall be generated when a reasonability limit violation is detected, the value shall be marked with a "reasonability violation" quality code, and the value shall be processed as for a telemetry failure. When the data returns to a reasonable value, the new value shall be accepted, the "reasonability violation" quality code shall be removed, and a return-to-normal alarm shall be generated.

18.3.2.4 Operating Limit Checking

All analog points shall be compared against operating limits that define various operating ranges for the point. Pairs of high and low limits shall be supported for each point (refer to Exhibit 15-4). The initial value of each limit shall be defined as part of the point's database definition. The TDMS shall ensure that the limit values obey the following relationship for every analog point:

Low reasonability limit ≤ low limit "n" ≤ ... ≤ low limit1 < high limit1 ≤ ... ≤ high limit "n" ≤ high reasonability limit

The TDMS shall enable users to override the value of any limit. Overridden limits shall be marked with a "limit override" quality code and shall be used in place of the initial limit value. When the user removes the override, the limit shall revert to its initial value. All overridden limits shall be presented on the alarm inhibit and override summary (refer to Clause 16.7.12.6) and the manual replace summary (refer to Clause 16.7.12.8).

It shall be possible for a user to mark any limit as inactive. Inactive limits shall not be checked. Marking a limit as inactive is not to be confused with inhibiting alarms (refer to Clause 16.4.6). Alarm inhibiting shall apply only to active alarms.

The “normal range” of an analog point is defined as the set of values between the innermost low and high limits. Whenever an analog value crosses a limit in a direction away from its normal range, a limit violation alarm shall be generated and the analog value shall be marked as being in the “off-normal” condition; however, analog limit violations that are the result of supervisory control actions shall be reported as events rather than as alarms. All analog points that are “off-normal” shall be included in the off-normal summary display (see Clause 16.7.12.3).

Whenever a monitored point crosses a limit in a direction towards its normal range, a return-to-normal alarm shall be generated. Whenever an analog point crosses more than one limit, each limit crossing shall be alarmed.

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 unique deadband shall be specified for each analog point.

18.3.2.5 Rate-of-Change Checking

Selected analog points shall be checked against rate-of-change limits. A rate-of-change limit shall be defined for every analog point subject to rate-of-change limit checking. An alarm shall be generated when the change in the value of the analog point between two successive scans exceeds the point’s rate-of-change limit. The check against the limit may be either against the absolute value of the change (where a violation is declared if the value is increasing or decreasing) or against a signed value (where a violation is declared only when the change in value is in the same direction as the sign of the limit) as selected for each checked point.

Rate-of-change alarming shall be inhibited for analog changes caused by supervisory control operations.

A user shall be able to override the limit values. Overridden limit values shall be marked with a “limit override” quality code. When the user removes the override, the limit shall revert to its initial value.

A user shall be able to mark the rate-of-change limit as inactive. An inactive limit shall not be checked.

Whenever a rate-of-change alarm has been declared for an analog point, the point shall be marked as being in the “off-normal” condition. All analog points that are “off-normal” shall be included in the off-normal summary display. As soon as the change in the analog’s value is less than the rate-of-change limit, the point shall be removed from the off-normal summary display.

18.3.2.6 Operating Limit Sets

The TDMS shall support operating limit sets. As in Exhibit 15-8, the quantity of operating limit sets or pairs to be supported is three (3). Each operating limit set shall include an entry for each operating limit in the database. Upon user command, the current operating limits for an individual point or for all points in the TDMS shall be overwritten with the corresponding entry from the selected operating limit set. The TDMS shall not overwrite a limit that is marked as manually overridden. Instead, the point and limit with the conflict shall be listed on a limit conflict display. This display shall identify the point and

limit, along with the value of the initial (non-overridden) limit, the value of the override limit, and the value of the limit from the operating limit set.

18.3.3 Equipment Status Data

Prior to storage in the TDMS database, equipment status data shall be processed to convert the input data to a meaningful state and to identify and report changes in state.

18.3.3.1 State Conversion

The TDMS shall include state conversions where two-state points, typically reported as a single status bit, represent one of two possible states of a power system device or other equipment or process. Any value of the input shall be converted to any defined state for the point. For example, the TDMS shall support at least two-state conversions that correspond to open/closed, trip/close, on/off, alarm/normal, auto/manual, and remote/local. The Authority shall define the state definitions. The assignment of the value conversion and state definition shall be made on a per-point basis.

The TDMS shall also process all reported changes of any device where multiple changes are transmitted in the same message.

18.3.3.2 Normal State Processing

One of the states of each status point shall be designated as its “normal” state. The designation shall be made individually for each point. It shall also be possible to define a point as having no normal state. Users shall be able to override the normal state definition and to remove the override. Overriding the normal state designation shall establish a “normal state override” quality code on the point. Removal of the normal state override shall remove the normal state override quality code. All points with an overridden normal state shall be listed on the off-normal summary display (Clause 16.7.12.3).

18.3.3.3 State Change Detection

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. Changes in state that are the direct result of a supervisory control action initiated via the TDMS shall be reported as events. Spontaneous changes in state (changes that are not the direct result of a supervisory control action) shall be reported as alarms.

All status points that have a normal state designated and whose state is not the normal state after a state change shall be included in the off-normal summary display.

18.3.4 Accumulator Data

Prior to storage in the TDMS database, accumulator data shall be processed as follows:

1) Conversion to engineering units

2) Reasonability checking

3) Limit checking

4) Accumulator substitution.

18.3.4.1 Conversion to Engineering Units

Data sources will report accumulator points in two forms, as a continuous count value and as a resetting count value. These Technical Specifications consider accumulator values collected from data sources that have been processed by the data source to be a form of resetting count values. That is, even though the value may have been converted to engineering units and checked for limit violations prior to transmission to the TDMS, the TDMS shall process the value as if it had not been previously processed. This will, for example, enable the TDMS to convert kWh values to MWh values, and to check the value against different limits.

Data reported in raw count form shall be converted to engineering units using the following linear conversion equation:

$$Converted\_value = a*(Raw\_value_n – Raw\text{-}value_{n-1})$$

where *a* is a scaling factor, Raw_value_n is the current telemetered value, and Raw_value_{n-1} is the previous telemetered value. The coefficient may be of any sign and shall be individually defined for each accumulator value.

The Authority will specify the maximum and minimum count value for each accumulator point. The conversion shall accommodate accumulator rollover. That is, when the raw value reaches it maximum value and rolls over to its minimum value.

Data reported in resetting count form shall be converted using the following linear conversion algorithm:

$$Converted\_value = a*(Raw\_value_n)$$

where *a* and Raw_value_n are as defined above. Raw_value_n will be reset to zero after it has been successfully read from the data source.

Each component of the accumulator value, including the current and previous (if applicable) raw values and the converted value, shall be stored in the TDMS database. The Authority prefers an implementation that stores the raw value(s) in count form and the converted value as an analog value.

18.3.4.2 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.

An alarm shall be generated when a reasonability limit violation is detected, the value shall be marked with a reasonability violation quality code, and the value shall be processed as for a telemetry failure. When the data returns to a reasonable value, the new value shall be accepted, the “reasonability violation” quality code shall be removed, and a return-to-normal alarm shall be generated. The TDMS shall provide the ability for the Authority to change the high and low reasonability limits, which shall be unique for each point.

18.3.4.3 Operating Limit Checking

All accumulator points shall be compared against high and low operating limit pairs (refer to Exhibit 15-4). The initial value of each limit shall be defined as part of the point's database definition. Users shall be able to override this limit value. Overridden limits shall be marked with a "limit override" quality code and shall be used in place of the initial limit value. When the user removes the override, the limit shall revert to its initial value. Limits (both initial and overridden limits) shall be constrained to be within the reasonability limits of each accumulator point.

A user shall be able to mark any initial limit as inactive. Inactive limits shall not be checked.

The "normal range" of an accumulator point is defined as the set of values between the low limit and the high limit. Whenever an accumulator value crosses a limit in the direction away from its normal state, a limit violation alarm shall be generated and the accumulator value shall be marked as being in the "off-normal" condition. All accumulator points that are "off-normal" shall be included in the off-normal summary display.

Whenever a monitored point crosses a limit in the direction towards its normal range, a return-to-normal alarm shall be generated. The return-to-normal alarm message shall contain the same information as a limit violation alarm message except that it indicates that the alarm region has been exited.

18.3.4.4 Long Value Accumulator Quality Code

As described in Clause 18.1.7, the value of a telemetered accumulator point is not acquired because of a telemetry failure, the point shall be marked with a "telemetry failure" quality code.

Generally, during periods of telemetry failure, the accumulator continues to collect data. The first time the data source reports continuous count accumulator data after data acquisition is restored, the reported value will represent the accumulation of the whole period of failure, and not just the most recent period of accumulation. Consequently, the first value of accumulator data acquired after the restoration of data acquisition shall be marked with a special "long value" quality code.

18.3.4.5 Accumulator Substitution

The TDMS shall support the substitution of other data for invalid accumulator values. The substitution shall be triggered by any of the following conditions:

1) Telemetry failure of an accumulator point

2) An accumulator point with a long value quality code

3) 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"). The Authority shall specify, for each accumulator value, the association between the accumulator value and the other value and the maximum difference value.

Note that the accumulator value may be the result of redundant data processing (Clause 18.3.8). To ensure that the redundant data processing completes prior to the accumulator substitution processing, accumulator substitution processing shall be delayed by 15 seconds from the completion of the accumulator value conversion and storage of the converted value in the database. Note also that an accumulator value that has been manually entered by a user shall be considered a valid value.

The value to be substituted shall be selected by the Authority for each point from any of the following:

1) A calculated or telemetered accumulator value

2) A calculated or telemetered analog value

3) A value of zero (0).

Only a single substitution value will be selected for any point. That value shall be substituted only if its quality codes indicate a current and valid value. (Values outside alarm limits shall be deemed valid.) If the substitution value is not current or not valid, a zero value shall be substituted. This substitution shall occur in lieu of retaining the last good value as defined for telemetry failure. Substituted values shall be marked with a suitable quality code, in addition to a telemetry failure code and distinguishable from the redundant data processing quality code.

18.3.5 Sequence of Event Data

This data shall be stored in the IS&R function (Clause 19) for presentation on displays and reports. Refer also refer to Clause 18.1.8.

Certain data in the database will not be updated from data sources or TDMS functions, but will be manually entered by users. These data points shall include analog, accumulator, and status points.

Event messages shall be generated for each change made to a non-telemetered value. Non-telemetered points shall be marked with a “non-telemetered” quality code, but not with a “telemetry failure” quality code or a “manual entry” quality code. Non-telemetered points shall be otherwise indistinguishable from telemetered or calculated points.

18.3.6 Calculated Data

Calculated points shall be derived from Authority-defined algorithms (generalized calculations) and pre-defined algorithms supplied with the TDMS (such as MVA calculations and analog value integration). Typically, such calculations will be performed periodically. The periodicity of the calculations shall be assigned on a per-point basis. An implementation is also required where a calculation is triggered whenever any of the arguments of the calculation change. In this case, the execution periodicity shall be interpreted as the maximum allowable time from the change of the argument until the calculation is completed and the result is stored in the database.

The user shall be able to suspend and enable the calculation of any calculated data point. A “calculation suspended” condition shall be set for any point for which the calculation was suspended.

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 TDMS functions. The Authority prefers an implementation in which analog and accumulator calculations produce results that can be stored as either analog or accumulator values.

The calculation function shall detect arithmetic exceptions such as division by zero and over-range results. Such conditions shall place a "calculation failure" quality code on the resultant calculated point. (This may also be represented by a "telemetry failure" quality code.)

The TDMS shall support user entry of a substitute value for the results of any calculation. The resulting value shall have a manual substitution quality code.

18.3.6.1 Generalized Calculations

Generalized calculations shall be defined from the following operators and rules:

1) *Mathematical operators* – addition, subtraction, multiplication, division, absolute value, square root extraction, exponentiation, and logarithmic functions

2) *Trigonometric functions* – including sin, cos, tan, and inverse functions

3) *Summation function* – summation of "n" different variables

4) *Daily totals function* – the daily total of hourly values for a single variable

5) *Average function* – average of the values for a single variable over predefined intervals, such as one hour

6) *Filter function* – digital filter in the form $\alpha * x + (1- \alpha) *$ (previous filtered value)

7) *Min/max functions* – selection of the minimum and maximum value from a set of arguments

8) *Peak function* – determination of the maximum values for a single variable over predefined intervals, such as maximum over one hour and hourly maximums over one day. Peak determinations shall also save the date and time of occurrence.

9) *Logical operators* – including AND, OR, NOT, and XOR

10) *Comparative operators* – including greater and less than, equal to, and combinations thereof

11) *Value limiting functions* – zero cutoff, high limiter, and low limiter

12) *Conditional execution operators* – including if-then-else statements.

Each calculation may consist of up to ten arguments. Multi-level parenthesis shall be supported. It shall be possible to use the quality codes of database values as arguments.

The TDMS generalized calculation shall support the capability to drag and drop points from displays or the database into the calculation definition. Examples of typical calculations are presented in the following sub-clauses.

18.3.6.2 MVA Calculation

MVA shall be calculated using any of the formulas specified below. The formula to be used shall be selected for each MVA calculation.

1) $MVA = \sqrt{MW^2 + MVAr^2}$ – sign always positive

2) $MVA = \sqrt{MW^2 + MVAr^2}$ – sign same as sign of MW

3) $MVA = \frac{kV * A * \sqrt{3}}{1000}$ – sign always positive

4) $MVA = \frac{kV * A * \sqrt{3}}{1000}$ – sign same as sign of A (Ampere).

18.3.6.3 Integration

The integration calculation will typically be used to produce MWh and Mvarh values from MW and Mvar inputs respectively. 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. Two values shall be maintained in the database as analog values for each integration point:

1) The *current value* – the value for the current (in-progress) period

2) The *previous value* – the result for the previous (completed) period.

Each integration point shall be recomputed each time the argument is scanned and the argument is judged to be valid (refer to Clause 18.3.1), i.e., the current value shall be recomputed to reflect the integrated value at the time of the sample. A count of valid samples for each integration point shall be maintained through the integration period. The count shall be compared against an Authority-entered minimum count for each point at the end of the integration period. If the count of valid samples for a period is below the minimum value, a calculation failure shall be considered to exist and the (calculated) current value shall be stored with the “calculation failure” quality code. The count shall be reset at the expiration of each period.

18.3.6.4 Processing of Calculated Data

After a data item is calculated, it shall be processed as follows:

1) Analog value:

    a) Reasonability limit checking (Clause 18.3.2.3)

b) Operating limit checking (Clause 18.3.2.4)

c) Rate-of-change checking (Clause 18.3.2.5).

2) Status value:

a) Normal state checking (Clause 18.3.3.2)

b) State change checking (Clause 18.3.3.3).

3) Accumulator value:

a) Reasonability checking (Clause 18.3.4.2)

b) Operating limit checking (Clause 18.3.4.3).

18.3.7 Not-Commissioned Data

The not-commissioned attribute is used to indicate equipment that is being commissioned into service. A unique "not commissioned" quality code shall identify all such equipment on any TDMS display or report and this quality code shall be applied/removed by the user (typically by maintenance staff). A user shall be able to declare individual data points or a data source as not-commissioned. In the latter case, all data points within that data source shall have the not-commissioned attribute applied.

18.3.8 Redundant Data Processing

Selected values in the TDMS database may be obtained from more than one source. Typically, the "best available" source of the value is chosen for use in displays, reports, and other functions. The function of choosing the best available source is called "redundant data processing." Any redundant value used other than the normal source shall be marked with a redundant value quality code.

The redundant data processing inputs are called "arguments", and the chosen source is called the "resultant best value." The arguments may include telemetered values, calculated values, and values generated by TDMS functions. The resultant best value shall be stored in the TDMS database.

Generally, the arguments and the resultant best value will be the same database type. However, it shall be possible to use both analog and accumulator values as arguments for an accumulator resultant.

When defining the calculation for a resultant best value, the user will rank the arguments in a priority order. The resultant best value shall be determined by selecting the "best available" from among the arguments. The highest-ranking argument with a valid value (see Clause 18.3.1) shall be stored as the result. If none of the arguments have a valid value, the highest-ranking item with the best quality shall be stored as the result. The TDMS shall allow the Authority to define the ranking of the quality codes for redundant data processing.

Users shall be able to override automatic selection and manually select any argument. Restoration of automatic redundant data processing shall require manual action by a user. Automatic and manual changes of the selected argument shall be reported as an event.

18.3.9 Network Status Data

The energized/de-energized state and the in-service/out-of-service state of each power system element shall be determined and stored in the database as status points. These status points shall be used so that the Dispatcher, for example, can be kept informed of the energized/de-energized and in-service/out-of-service states of the power system elements via SCADA one-line displays without the need for any input from the Dispatcher. Any changes to the power system shall be automatically reflected in the network status calculation.

18.3.9.1 Determination of Energization Status

A circuit element (transmission line, bus section, or distribution line segment) shall be considered energized if one of the following conditions exists:

1) There is a non-zero measurement of voltage associated with the element

2) A breaker or switch at either end of the element is closed and the adjacent section is energized.

A power system device shall be considered energized if it is connected to an energized circuit element or power system device.

Energization shall be treated as a calculated status point, and as such, the data quality of the arguments shall be propagated to the result.

If the TDMS identifies a contradiction in calculating circuit energization (for example, a circuit element is isolated but is associated with a non-zero voltage measurement), it shall issue an alarm identifying the contradictory database point and shall set an inconsistent result quality code for the energization.

18.3.9.2 Determination of In-Service Status

A circuit element shall be considered in-service if it is conducting power. Any circuit element that is energized and connected to a load shall be considered “in-service.” It is to be noted that an energized circuit element may be out-of-service as would be the case, for example, if one end were connected by a closed switch to another energized segment, but the switch at the other end were open.

18.3.10 Operations Monitoring

The Operations Monitoring function shall track the number of operations made by every breaker, capacitor switch, recloser, and load break switch that is monitored by the TDMS. 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.

Each monitored device shall be associated with a total operations counter. This counter shall be incremented whenever the associated device changes state. When a field device interface reports a multiple change (such as a trip-close-trip sequence), each transition shall be counted separately. The date and time of the last operation shall be saved for each device when one of the counters is incremented.

A Dispatcher with proper authorization shall be able to enter a total operations limit for each counter. An alarm shall be generated when a counter exceeds its limit. No additional alarms shall be generated if the counter is incremented again before it is reset. For each counter, the TDMS shall calculate the present number of operations expressed as a percent (which may exceed 100%) of the corresponding limit.

The ability to reset individual counters shall be provided. In addition, a user shall be able to inhibit operations counting for individual devices. Such devices shall be included in summaries based on areas of responsibility. Resetting and inhibiting counters shall be permitted only for devices that belong to the areas of responsibility to which the workstation is assigned, and resetting shall require the workstation to be assigned to an appropriate mode of authority. The date and time when each counter was last reset shall be saved.

The counters and other related information shall be available for display and inclusion in reports. 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.

18.3.11 Feeder Outage Statistics

The TDMS shall maintain feeder outage statistics expressed in the form of performance indices such as SAIDI, SAIFI, CAIDI, and MAIFI, which shall provide a standardized measure of the reliability of the Authority's distribution network with respect to the frequency and duration of unplanned outages whether sustained or momentary. The calculation of these performance indices shall be based on the IEEE 1366-2003 standard. The indices shall be calculated using a batch process that can be executed at regular specified intervals or on-demand.

The performance indices shall be included in feeder reliability reports. They shall be capable of being reported on a time interval basis such as month-by-month and annually. In each case, they shall be broken down by Authority service territory, region, and area.

It shall be possible for the user to exclude outages that may occur, for example, because of major storms.

18.4 Equipment Outage Scheduling

The Contractor shall provide an Equipment Outage Scheduling (EOS) function that will allow the Dispatcher to pre-schedule power system equipment maintenance outages and any necessary changes to power system equipment ratings due to such outages. The outage schedules shall be accessible to all application functions requiring the status of network equipment in the future or in the past.

The Dispatcher shall be able to easily enter, review, and modify schedules using interactive displays. Use of device codes and numbers for entry of schedules are unacceptable. In addition, the Dispatcher shall not be required to type in all fields defining the outage schedule except for de-rated values.

As a minimum (i.e., allowing for adjustments during project implementation), an equipment outage schedule shall consist of the following:

1) Category (HV or MV equipment).

2) Device type (line, transformer, circuit breaker, line recloser, line recloser/regulator, shunt capacitor, var controller, remote controlled switch, etc.).

3) Device name.

4) Planned Start date and time.

5) Planned End date and time.

6) Actual Start date and time.

7) Actual End date and time.

8) Generation or transformer deration (where applicable).

9) Dispatcher comments in English and/or Thai.

The Dispatcher shall be able to readily establish a default schedule by selecting the device name or symbol on the tabular displays and/or one-line diagrams. Upon selection, EOS shall establish a default schedule for the device and automatically call up the schedule entry display.

The last entry in the schedule list shall be the newly entered default schedule. The schedule shall include the device name, device type, a default start date and time that shall be the instant of selecting the equipment for outage, a default end date and time that shall be open ended. If the device is a generator or transformer, a default de-rated limit equal to the device's high operating limit shall be entered. The Dispatcher shall be able to modify the default start/end date and time and the de-rated limit or delete the schedule. EOS shall allow schedules to be entered up to a pre-defined time of at least 3-months into the future.

Displays that summarize the existing schedules by device type and in start date/time chronological order shall be provided. It shall be possible to order the outage schedule list by any of the available fields or device categories.

Upon the planned start and completion of an outage schedule, an event shall be generated to notify the Dispatcher. The Dispatcher shall have the option of modifying the comments, entering the actual start or completion time or alternately rescheduling the outage. The changes, including the ID of the Dispatcher making the changes, shall be recorded with the outage data for later audit. EOS shall store all previous day outages as past outages. The expired outages shall be purged automatically from the active outage list and placed into the previous day's outage list at midnight. The starting and stopping of outage schedules shall be recorded in the IS&R database.

18.5 Tagging

Tags are conditions applied to database values to call user attention to exception conditions for field device interfaces and to inhibit supervisory control actions.

18.5.1 Tag Types and Supervisory Control Inhibit

The TDMS shall support the number of tag types and the number of tags to be set on an individual point basis (also refer to Exhibit 15-8). The Authority shall order each tag type to indicate its relative priority to other types.

The tag types shall be defined to correspond with the Authority's field device interface tagging. The definition shall include the tag type name (such as, warning, caution, hot line, and do not operate) and any of the following user selected control-inhibit properties:

1) All control allowed.

2) Control inhibited in one direction, such as close.

3) Control inhibited in the other direction, such as trip.

4) All control inhibited.

The supervisory control function shall check for the presence of a control-inhibit tag as part of the control permissive scheme defined in Clause 18.6.7.

18.5.2 Tag Application

It shall be possible to apply a tag to any database item. A user shall place tags by selecting the database item to which the tag is to be applied and by then selecting a tag menu command. The user shall be required to enter, for each tag, the following information:

1) Date and time of tag placement.

2) Tag type.

3) Substation and point identification (supplied by the TDMS).

4) Comment. As part of the tag placement process, the TDMS shall prompt the user to enter alphanumeric comment information to be stored with the tag. The comment field shall be at least sixty (60) characters in length.

5) The ID of the user applying the tag. Each tag shall be uniquely identified with the user who placed the tag. This user identification shall occur automatically by attaching the user login name in the user assignment field (also refer to Clause 16.3.20.1).

Each tag shall be presented on a tag summary display. The display shall order the tags by substation. A user shall be able to edit and delete tags from this display. Tag application and removal shall be recorded as events. Each database item presented on a display shall have an associated attribute to indicate the highest-priority tag applied to the item. Devices with multiple tags shall be identified. Selection of the device tag shall bring up the tag summary display.

18.6 Supervisory Control

The TDMS shall issue supervisory control commands to field device interfaces when directed by a user or an application program. Control actions requested by a user shall include a confirmation step after selection of the field device interface to be controlled and the control action to be commanded. After the user confirms the control action, the supervisory control message exchange process shall be initiated. The message exchange with the field device interfaces shall use a select-checkback-execute command sequence. 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 interface and control action have been selected. 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.

If, after selecting a field device interfaces and control action, the user does not execute the control action within 20 seconds (a programmable interval) or if the user performs any workstation action other than executing the control action, the selection shall be cancelled and the user informed. The user shall not be prevented from requesting other displays, performing a different supervisory control action, or performing any other operation while the TDMS waits for a report-back on previously executed control actions.

18.6.1 Single State Control (Relay Reset)

The TDMS shall support the supervisory control of devices, such as underfrequency reset relays, that can only be commanded to one state. It shall not be possible to select a command into a second state for these devices.

18.6.2 Two State Control (Switching Devices)

This includes controllable switching devices such as circuit breakers, recloser relays, load break switches, and motor-operated disconnect switches.

It also includes control points that are designated as “delayed close” points, as in capacitor bank switching, where any supervisory control action shall be inhibited for a specified interval after the switch has been opened. The interval shall be determined by the Authority and specified individually for every device subject to delayed closing. If a user attempts to operate the device prior to expiration of the time interval, the error shall be managed as a permissive check failure (Clause 18.6.7).

18.6.3 Incremental Control

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.

The control of the device for a raise/lower operation shall follow the same sequence as for switching device control that uses a select-checkback-execute command. However, once selected, it shall not be necessary for the user to reselect the device for additional raise/lower operations; the user shall only have to apply the desired number of raise/lower execute commands, which shall be performed immediately. The user shall be able to cancel the operation at any time. The TDMS shall cancel the

operation twenty (20) seconds after a control execute has been issued or if the user performs any workstation action other than the control execute command. The timer shall be reset with each subsequent control execute command. The data acquisition function shall not be suspended between the times that repeated raise/lower execute commands are issued. Control actions that would result in movement of the device beyond its defined operating range shall be rejected (i.e., if a position feedback value is telemetered).

18.6.4 Set Point Control

The TDMS shall provide the capability to issue set point control to field equipment and to other computer systems. With set point control, the TDMS shall transmit a numerical value to the device being controlled, to indicate the desired operational setting of the device.

18.6.5 Automatic Supervisory Control

The Automatic Supervisory Control (ASC) function shall permit multiple supervisory control commands to be programmed for automatic execution in a predefined sequence.

Commands to be supported shall include:

1) All supervisory control commands.

2) Pause execution for a given time delay.

3) Stop execution until a user commanded restart or continue.

4) Conditional check before execution.

5) Jump (pass control to another ASC sequence).

6) Manual entry.

After executing a supervisory control action, the TDMS shall pause to obtain an indication of a successful control completion check (see Clause 18.6.6). If the control completion check is not received, or does not have the expected value, the TDMS shall terminate the execution of the ASC sequence and shall declare an alarm. 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 TDMS shall not introduce any artificial delays in the execution of an ASC command sequence.

No limit shall be placed on the number of ASC command sequences, which may execute in parallel.

The following manipulation of ASC lists shall be possible:

1) Display a catalog of the lists.

2) Display, build, copy, edit, and delete a list.

3) Name the list and enter a description.

4) Store the list.

5) Select the list for execution.

6) Execute the list.

At any time during the execution of a list, the user shall be able to stop further execution via an ASC cancel feature.

In addition, telemetry and control permissive checks shall be incorporated in the sequence with user override capability. Upon failure of the telemetry and control permissive checks, the ASC sequence shall pause and require user interaction. Resumption of the ASC sequence at any point shall be provided.

Initiation of any ASC 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 completed shall also be recorded as events.

If the user is using a list to perform a repetitive function, such as issuing set points, the user shall be allowed to inhibit event messages for the sequence.

18.6.6 Control Completion Check

The response to all control actions shall be verified by monitoring a feedback variable designated individually for selected control points. If a feedback point is not defined for a control point, the control completion check shall be deemed successful if the control command is successfully transmitted to the field device interface. A report-back timer, independently defined for each device, shall be started when the execute command is issued. Each delay time shall be adjustable from two seconds to at least ten minutes to a one second resolution.

The user shall be provided with an indication that a control action is in progress, and a report of the result of the control action. A control action shall be deemed successful if the appropriate success indication described below is recognized prior to expiration of the report-back timer:

1) 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. Even if the change is momentary, the control action shall be reported as successful. The data acquisition and processing functions shall then report the subsequent change away from the controlled state as an alarm.

2) For *incremental control devices* – the corresponding analog feedback point of the device under control changes to the desired value, within a tolerance, individually specifiable for every device

3) For *set point outputs* – the corresponding analog feedback point of the output under control changes to the desired value, within a tolerance, individually specifiable for every device.

Successful controls shall be recorded as an event. If the control was unsuccessful, an alarm shall be generated. The alarm shall differentiate between failures due to communications problems and failures of the device to achieve the desired end state.

For supervisory control commands issued as part of a group control or load shedding operation (Clause 18.7), the successful completion of all control actions shall be reported via a single message. If any operation is unsuccessful, the user shall be informed of those devices in the group that failed to operate by individual alarms.

Where a supervisory control action is initiated by an application via the programming interface, the interface shall include features to report the success or failure of the control action to the application. Also, refer to Clause 8.1.

18.6.7 Control Permissive

The supervisory control function shall perform a permissive check immediately after the user has selected the device and control action. The presence of any, all, or none of the following conditions for the selected point shall be deemed as a failure of the check:

1) The feedback point for the control point is in the state to be realized by the control command.

2) A status value from the TDMS database, designated for each controllable point, evaluates as true.

3) A tag with a supervisory control inhibit property is set.

If the permissive check fails, the user shall be informed of the failure by a message that clearly indicates the permissive failure and that differentiates among the check types. The user shall be presented with the options of canceling the control action and of overriding the permissive. If the user elects to override the permissive check, the message presented for the execute step and all records of the control action shall clearly indicate that the user has overridden the permissive check.

If the permissive check passes, the select-checkback-execute control sequence shall then proceed to completion.

Where a supervisory control action is initiated by a Contractor or Authority-supplied application via the programming interface described in Clause 8.1, the interface shall include features to report the presence of a control inhibit tag and to accept override commands from the application.

18.7 Load Shedding and Restoration

A load shed and restore function shall be provided. This function shall execute on demand by any Dispatcher responding to a directive indicating the amount of load that should be shed or restored within the Dispatcher’s AORs. Once initiated, the function shall proceed to remotely open and close feeder breakers automatically to achieve the load shed target set by the Dispatcher. The response time of the function shall be governed by the speed with which the individual supervisory control actions can be implemented.

The function shall consist of four packages:

1) Underfrequency relay monitoring

2) Fixed load shed

3) Rotational load shed

4) Restore.

The results of any load shed operation shall be archived in the IS&R (see Clause 19).

18.7.1 Underfrequency Relay Monitoring

The TDMS shall include a function that monitors the Authority's underfrequency relays. The underfrequency relays are set to operate whenever the frequency drops below the pre-set stages for each relay. The TDMS shall support up to 10 stages.

The underfrequency relay monitoring function shall monitor the MW flows through the relays before and after the shedding. The monitoring before load shedding shall include monitoring feeders subjected to load shedding, and summing up the MW flows to form the system totals for each load shedding stage. These totals shall be displayed, smoothed, and updated every scan cycle. In addition, the display shall contain the available load to be shed both in MW and as a percentage of the area's total system load. Displays shall be provided to allow the user to view the devices associated with each underfrequency relay.

The underfrequency relay monitoring function shall, upon load shedding, verify that the proper devices were operated when an underfrequency relay trips. The function shall record the amount of load tripped by the relay and alarm any device that should have tripped, but remained closed.

18.7.2 Fixed Load Shed

Using the fixed load shed, users shall manually command the shedding of blocks of load. A "load block" is a predefined set of feeders whose feeder breakers may be opened when it is necessary to shed load. Displays shall be provided for interactive definition and review of load blocks. The fixed load shed function shall also monitor the load (in MW) of the total system, the load of load blocks, and the load of individual feeders within the load-shed block.

The user shall be able to manually shed an entire block of load by selecting the block and executing a load shed command. The fixed load shed function shall then automatically command opening of appropriate breakers in sequence. An option shall be available to stagger openings of breakers involved in a block shedding. The amount of time used in staggering shall be user-enterable. The users shall be able to shed an entire block or individual loads within the block.

18.7.3 Rotational Load Shed

The TDMS shall include a rotational load shedding function. Each load subject to load shedding is assigned to one of the load blocks. Individual feeders within each block are assigned a priority, and an

ordered list of the feeders is maintained for each block per their priority. Each feeder shall have a parameter associated with it that indicates the maximum amount of time that the feeder load may be shed.

The Contractor is required to provide interactive displays for maintaining this list, and for displaying and prioritizing individual breakers within the blocks. The displays shall also show total system load, an estimate of unserved load, the duration of the load outage for each feeder, actual MW flows through the breakers comprising each block, a total MW of each block, customers affected, and an alarm indicator whenever the load available for shedding in the current time interval and for the current day falls below the required load shedding range.

The rotational load shedding function shall provide appropriate displays and the functionality to allow a user to enter the amount of load to be shed in either of the following ways:

1) As a certain amount of MW.

2) As a percentage of the total load available.

3) As a replacement for the load shed by the underfrequency relays.

The TDMS shall determine the number of groups and loads within each group that must be shed to achieve the load shed requirement and shall open the corresponding breakers in prioritized sequence. The TDMS shall automatically switch to the next energized load in the group whenever a load in the group has been shed for the maximum allowable time. The rotation of loads shall maintain approximately the same level of load shed for each group while equalizing the amount of time that loads within a group are disconnected. The rotating load shed function shall continue until terminated by the user.

18.7.4 Restore

The restore function shall allow the user to restore load that has been shed by the load shed function. The user shall be able to restore the load either individually or as a group via interactive display commands. An option shall be available to stagger closing of breakers involved in a block shedding. Displays for showing unserved load shall be provided with a capability to sort by the estimate of unserved energy, by the duration of the outage for each breaker, by blocks, and by priority. These displays shall also display the total system load and an estimate of the total unserved load.

18.8 Switching Management System

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. Thus, the TDMS shall include a Switching Management System (SMS) application to support the manual creation, automatic creation, execution, display, modification, maintenance, and printing of switching orders. This shall include the ability to define time delays and breakpoints as part of switching orders.

The switching order software shall support switching order life cycles and user privileges. A switching order life cycle, for example, shall consist of a sequence of switching order states or stages such as

submitted (proposed), scheduled, prepared, checked, authorized, rejected, postponed, active, on-hold, terminated, and completed. All incorporated switching rules shall be compliant with the Authority's rules. The SMS software tools shall allow the user to easily create and/or modify such rules.

After creating a switching order, the user shall be able to have it saved and exported in a standard file format.

Once defined, the Dispatcher shall be able to execute a switching order in real-time mode and in study mode. The study mode shall allow the user to check out the switching order's potential impact on the power system prior to actual execution.

18.8.1 Manual Creation of Switching Orders

The user shall be able to create a switching order by using a full monitor editor to enter information for the header and the body of the switching order. Preparation of the switching order, in the form of a list of actions to be performed, shall require as little user interaction as possible. This shall include the ability to start from an existing order and the ability to create or complete an order using, for example, power system device drag-and-drop selections from one-line schematic and/or geographical displays. In creating or completing an order, easy-to-use features such as the ability to enter tags and any other switching related action shall be provided.

The header of the switching order shall contain information such as the following:

1) Switching order sequential number
2) Authorization number
3) Work order number
4) Circuit name
5) Permit required (Yes/No)
6) Start date and time
7) Completed date and time
8) Scheduled times of forward and reverse switching orders
9) Crew ID (e.g., service car number and crew names)
10) Nature of work
11) Location of work
12) Prepared by whom and when
13) Checked by whom and when

The body of the switching order shall consist of multiple entries defining the actions to be taken. Each entry shall have an entry number automatically assigned by the TDMS. 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.

When the user enters a switching order macro, the macro shall be automatically expanded to the full text. The user shall be able to edit the text of the macro expansion. In some cases, the user will need to fill in the blanks in the macro expansion to complete the entry.

The Authority will work with the Contractor to determine the exact form and content of the switching order headers and macros during project implementation. Printouts shall be possible using the MSOffice software to be provided with the TDMS. Documentation corresponding to the Authority's existing SMS application will be made available.

18.8.2 Automatic Switching Order Creation and Execution

The user shall be able to initiate the automatic creation and execution of a switching order that will reconfigure lines, buses, or feeders in accordance with the rules supplied by the Authority. Recognition shall be given to relevant interlocking schemes and the switching orders that will be generated by the Fault Location, Isolation, and System Restoration function (Clause 20.18). Typical rules used by the Authority shall include, but shall not be limited to:

1) Limiting overloads on fault restoration

2) Secondary transfers to non-adjacent feeders when there is insufficient capacity for load restoration

3) Minimizing switching actions

4) Prioritization of loads that will be affected by switching orders

5) Consideration of future loading of the network as well as current loading when performing switching operations.

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 transmission line, bus, feeder, or feeder sections to be reconfigured (i.e., disconnected or reconnected) and then request the TDMS to automatically create and execute the appropriate switching operations.

If desired, the user shall be able to review the switching operations created by the TDMS, make any necessary changes, and then request their automatic execution. Each switching operation shall be listed in the order in which the switching devices need to be controlled (tagged, opened, closed, etc.).

18.8.3 Automatic Generation of Back-Out Order

Most switching orders are created to perform temporary work. When the work is completed, there is often a requirement to restore or back out the circuit to normal conditions. This is frequently the opposite procedure from the one used initially.

The TDMS shall provide a mechanism to automatically generate a back-out switching order. Starting from an initial switching order, when the user requests "Generate Back-Out Order", the TDMS 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. For example, an entry CLOSE BREAKER shall be reversed to OPEN BREAKER, and an entry PLACE TAG shall be reversed to REMOVE TAG. The ultimate list of "reversible" entries and their associated "opposites" shall be developed in coordination with the Authority during project implementation. The user shall be able to edit the text of the various entries. Before the user is permitted to save the back-out order, the TDMS shall prompt the user to edit its header.

18.8.4 Maintenance of Switching Orders

After creating a switching order, the user shall be able to have it saved. The TDMS 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.

The TDMS shall maintain a directory of switching orders, organized by area of authority. 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.

The TDMS shall also maintain a file of switching order macros organized by authorized user name and sorted alphabetically. The user shall be able to add, delete, and modify the macros in this file per the user's assigned areas of responsibility. 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.

18.8.5 Switching Order Execution and Checkout

Once defined, the Dispatcher shall be able to execute switching orders (including back-out orders) in real-time mode and in study mode. Execution shall take place in proper sequence automatically or in manual step-by-step mode based on assigned breakpoints. All built-in time delays and breakpoints shall be recognized. Alternatively, the user may temporarily assign new time delays and breakpoints.

As in switching order preparation, study mode execution shall allow the user to check out the switching order's potential impact on the power system prior to actual execution. For example, it shall be possible to verify whether a planned switching order will result in power system overloads and voltage problems. The new circuit configuration, the energization of the circuit segments, and the ampere and voltage values expected from the planned switching order shall be shown on study versions of the power system world-map displays using dynamic coloring to highlight all possible limit violations.

18.9 DAC Simulator Functions

As referenced elsewhere in these Technical Specifications, the Contractor shall provide portable DAC Simulators for ensuring each installed field device interface is SCADA ready prior to integration with the TDMS. This shall include checks to verify that the database of the field device interface under test is correctly mapped point-for-point with the SCADA database and that the field device interface supports all required functionality.

The DAC Simulator shall be capable of checking that any field device interface is SCADA ready by direct connection to the field device interface at site. In addition, it shall be able to confirm the SCADA readiness of the field device interface remotely, e.g., from any project site with necessary communications access.

In effect, each DAC Simulator shall include the basic SCADA functionality to be included in the TDMS main platform. During project implementation, the DAC simulator software shall be updated as may be necessary from time to time to match the latest version of the SCADA software.

The DAC Simulator (refer to Clause 17.16 of these Technical Specifications) shall consist of a notebook PC equipped with all necessary communications ports, adapters, cables, and connectors to communicate with the Authority's various field device interfaces. As a minimum, it shall contain:

1) Identical SCADA software for scanning or otherwise collecting data from every type of field device interface.

2) Identical SCADA software for data processing. This shall include the processing of all analog and status data types, as available in the database of every field device interface, along with all relevant alarm and event reporting capabilities.

3) Corresponding to each field device interface, the same SCADA database as the TDMS. This shall include both the telemetered and calculated points. To support the calculated points, the DAC Simulator shall include the SCADA calculation software (refer to Clause 18.3.6).

4) Identical SCADA software for checking the down loading and diagnostic features related to the field device interfaces.

5) For point-to-point testing of field device interfaces remotely, the necessary communications software as well as the necessary communication protocols (such as DNP 3.0 over IP).

6) Identical SCADA software for checking all supervisory control points associated with each field device interface. Refer to Clause 18.6.

7) Ability to import and export database and display definitions with the SCADA subsystem provided in both the Development System and TDMS.

8) SCADA related displays that appear to the user in the same way as they would when using the actual on-line SCADA system.

19. Information Storage and Retrieval

To support TDMS users located in the project's control rooms, Information Storage and Retrieval (IS&R) shall be executed as a redundant function in the TDMS Production Environment (PDE) at each data center. IS&R shall also execute as a non-redundant function in each data center's Pre-Production Environment (PPE). Any authorized, designated TDMS user shall be able to access all IS&R functions from any Contractor-provided TDMS workstation.

An instance of IS&R shall also be provided in the DMZE environment at each data center so that authorized, designated users on the Corporate WAN shall have synchronized, concurrent, but retrieve-only access to replicated IS&R functionality. Providing IS&R services to these non-TDMS users shall not affect the security of the TDMS from the perspective of the TDMS users. Thus, access by non-TDMS users shall be properly secured by Contractor-provided gateways consisting, for example, of routers and firewalls.

Depending on the proposed TDMS design, each IS&R instance shall execute on its own virtualized (Authority-preferred) or physical server.

Within this context, IS&R shall be capable of supporting a two or three-tier, i.e., client/server or client/application/server, architecture through the TCP/IP protocol. Open Database Connectivity (ODBC) is required with documented and demonstrable compatibility with Microsoft Access, Microsoft Excel, and other common front-end software. The DBMS shall be accessible by data management tools such as those based on Structured Query Language (SQL) and Dynamic Data Exchange (DDE). The Contractor shall provide the database client software and any additional Contractor-developed software that may be required to utilize the IS&R capabilities.

In general, any TDMS data value shall be available for capture, calculation, retention, and archiving by IS&R. This includes telemetered data, data received via data exchange such as ICCP, real-time calculated data, manually entered data, data quality codes and supervisory control tags, power system snapshots, and data used and produced by the TDMS applications, including savecases.

Data retrieval shall include on-line information query, display, trending, and reporting features along with an historical information playback function.

Some of IS&R's specific functions shall include:

1) Alarm and event capture, storage, and retrieval.

2) SOE capture, storage, and retrieval.

3) Periodic capture, calculation, storage, and retrieval of data required by pre-defined data sets.

4) Continuous data recordings of selected real-time data. This data shall not be capable of being modified.

5) Historical playback of the continuous data recordings.

IS&R shall also provide long-term archival storage and retrieval capabilities allowing subsequent analysis and other information processing to be accommodated. Thus, in addition to the memory sizing referenced in Clause 15, IS&R shall be provided with the on-line capability and capacity to extract and store data needed for a query that covers the maximum number of retention days for the highest periodicity data retained. It shall also be supported by all required archiving capacity.

Any third-party license(s) provided to support IS&R shall allow the Authority "full-use" of the software. It shall provide for Authority use of all databases and applications delivered with the TDMS

as well as permit the Authority to develop additional applications and/or databases generally related to the functionality of the TDMS.

19.1 General Capabilities

The general capabilities of IS&R are specified as follows.

19.1.1 User Access

User access to IS&R shall incorporate the following features as a minimum:

1) Menu driven data selection process.

2) Pre-formatted sets of data retrieval request displays built via the IS&R user interface.

3) Sets of generic routines for typical types of access, such as all analog points at a specific time and the average, maximum, and minimum of a value over a user nominated time period, application savecases, etc.

4) Capability to define *ad hoc* queries to call for any specific values that have specified similar characteristics over specified periods of time.

5) Capability to transparently deliver interpolated data for a specific time or period of time and associated periodicity, where the source is stored by exception.

6) Capability to display data graphically including *ad hoc* as well as pre-defined displays, such as user-specific dashboards.

7) Restrictions on access to confidential information based on user access control.

8) Seamless integration with typical Web browsers for user retrieval of IS&R data and for the presentation of reports.

9) Capability to retrieve any quality code, tag, or data value stored for any IS&R data value.

For retrieval purposes, it shall be transparent to requesting users or applications whether the requested information is stored on-line or on archival storage, or spans across both storage types. The IS&R shall satisfy a retrieval request for any time period and any time span. Sufficient relationships shall be maintained between the IS&R data and the TDMS Real-Time Data Base (RTDB) to ensure that selections can be made based on comparisons between stored IS&R values (such as a periodically saved bus voltage) and any related, fixed TDMS value (such as the bus voltage limit). In addition, displays shall be captured so that the data context can be maintained, e.g., savecases shall include model information and displays.

19.1.2 Function Access

The Contractor shall provide a library of programming interfaces to allow any function added by the Authority to access IS&R for information storage and retrieval. For example, the capability to initialize a power system network analysis study or simulation from IS&R for any date and time within a data

retention or archived period shall be provided. The data storage times closest to the date and time specified by the user shall be used to select values from the IS&R database.

The IS&R database shall also provide an interface to PC-based applications such as Microsoft Office applications (e.g., WORD, EXCEL, etc.), report generators, and other RDBMS and DBMS products via the latest standard SQL data requests or ODBC drivers.

19.1.3 Automated Data Capture

The capability to capture any analog, calculated, or status value defined in the TDMS database either upon detection of its change (with associated data quality codes and time tags) or periodically in sets of associated data shall be provided. Automated capture of alarms and events, user entries (including control, tag and flag requests, manual data entries such as limit changes) and system maintenance log entries shall be provided. All alarms and events shall be captured upon occurrence and forwarded to IS&R for storage and future retrieval.

The Contractor shall provide user-friendly forms that allow the user to build ad hoc queries of any combination of the individual fields stored with each entry. These fields shall include date, time, substation name, point name, alarm category, AOR, alarm priority, alarm type, data type, and message text. Queries may be saved and query results may be viewed, printed or written to a file in a format such as CSV, xlsx, txt, etc. In addition, each entry may have a user-entered comment.

Data shall be recorded in such a manner that it is possible to retrieve a complete view of the power system from any date and time specified by a user, i.e., a “snapshot.” The snapshot shall include all power system telemetered and derived measurements and status values (including quality codes, analog limits in effect at the time of the snapshot, etc.) as well as system alarm and events. The Contractor shall provide all tools necessary to retrieve this data using SQL and ODBC-compliant applications.

In addition to the above, the following types of data shall be capable of being stored and made available for user access:

1) Communications statistics and errors.

2) TDMS performance data.

3) TDMS server and function status.

4) Values of real power, reactive power, and line current (Amps) prior breaker and recloser trips.

5) Power application solution status for the different applications such as State Estimation (SE), Contingency Analysis (CA), Optimal Feeder Reconfiguration (OFR), Fault Location, Isolation, and System Restoration (FLISR), etc.

6) Selected power application analysis results.

7) Environmental data (e.g., weather, hydrological, etc.) data.

19.1.4 Data Quality Codes

The IS&R database shall include all of the quality codes associated with each point. In addition, a distinct quality code shall be provided to denote that a correction has been made to a point's value while in the IS&R database.

19.1.5 Data Calculation

IS&R shall provide the capability to perform calculations pre-defined by users on any captured data value at specified periodicities, when requested by a user, and when triggered by an application program. It shall also be capable of performing calculations on previously calculated data and, where data is captured periodically, of initiating calculations at the end of the capture period, i.e., after all required data has been obtained.

Calculations of the following types within a data set (corresponding to a user-specified snapshot in time) shall be supported:

1) Algebraic summation and subtraction
2) Add if positive or negative
3) Absolute value
4) Multiply, multiply if positive, or multiply if negative
5) Divide, divide if positive, or divide if negative
6) Square root
7) Exponential
8) Conditional testing (>, ≥, =, ≠, ±, ≤, <)
9) Boolean operations
10) Nested If, Then, Else
11) Trigonometry functions
12) Carry-forward (with and without integer truncation and carryover of the fractional value to the next time period).

Calculations of multiple samples (instantaneous values over time) of the same data point shall be supported. This shall include statistical measures such as the point's minimum, maximum, average, and total (accumulated) value for the following time periods for example:

1) 5, 15, 30, and 60 minutes using real-time samples.
2) AM and PM periods, where the Authority can define the hours in each period.

3) Daily using 15-minute samples.

4) Weekly using 15-minute samples.

5) Monthly using daily and 15-minute samples.

6) Yearly using monthly samples.

Calculated data shall include a quality code derived from the quality codes of the data used in the calculation. The quality code of the calculated data shall be derived in a similar fashion to the quality code of calculated real-time data points.

19.1.6 Data Storage and Retrieval

Data captured by IS&R shall be stored and made available to authorized users for viewing (including trending), inclusion in printed reports, exporting, archiving for long-term storage, and transmission to external systems. The selection of data for storage shall be controllable by the Authority, shall be defined in the RTDB, and shall not require separate IS&R definition.

The stored data, including archived data, shall contain sufficient information to enable the retrieval of the data value, its quality codes, and the time and date that the data was collected at any time in the future. Access to the stored data shall not be affected by TDMS failure and recovery, time change, or changes to the TDMS configuration. In addition, for example, the arithmetic precision of real-time data shall not be reduced when stored in the IS&R database.

All stored data shall be accessible from any time period regardless of any RTDB or IS&R database changes that may be made after storage of the data. For example, although the power system model may have changed, the capability to retrieve stored data for a variable that no longer exists in the TDMS RTDB and use it to initialize a network analysis function in study mode shall be provided.

Database changes shall not require stored data to be re-built (e.g., changing the IS&R database structure shall not require archived media to be re-built). This shall also apply to a retrieval request that may span across multiple database changes.

The addition, deletion, or modification of data to be collected and processed shall not result in loss of any previously stored data during the transition of data capture and processing to the revised database.

Users shall be able to select for retrieval any part, or all, of the data captured or processed by the IR&S for display, archiving, or any other purpose. This shall be supported by user-oriented procedures that do not require familiarity with database querying techniques. To display and print on-line IS&R data for specific points or predefined groups of points and for user-specified time periods, for example, procedures based on selection by pointing and minimal data entry shall be provided.

19.1.7 Data Editing

Authorized users may be permitted to edit IS&R data values. Such edited data shall be given a data quality of “Manually entered”. If the user manually edits any one or more of the component points of a calculation, the system shall re-compute the calculated value and its data quality. User-oriented manual

entry procedures shall be provided that do not require programming skills. All manual entry actions shall be logged. The system shall maintain a change log of who edits the data for audit purposes. The selection of editable data in the IS&R database shall be controllable by the Authority.

19.1.8 Off-Line Data Archiving

The TDMS shall be able to transfer IS&R data periodically to any removable storage medium for long-term archiving and for file transfer to other systems. Data older than its IS&R on-line retention period shall be transferred automatically.

The capability to restore archival data to the IS&R is also required. When archived data is restored, it shall be placed in a "reconstructed" file for use in the same way as IS&R on-line data. This shall not require removal of any IS&R on-line data, nor disturb the on-going IS&R data capture, storage, and retrieval process. User-oriented procedures, which do not require programming, or database querying skills, shall be provided to select the desired data and the particular time period data.

Selection of data for archiving shall be initiated by an authorized user. Pre-defined sets of data points and time periods to be copied and the destination device (if there is more than one) shall be selectable. More flexible selection of points shall also be supported. A user-oriented procedure is also required to delete reconstructed data files when they are no longer needed.

Data shall be archived in a format that is supported by commercial databases such as SQL.

19.1.9 Information Delivery

The Contractor shall provide enterprise information delivery tools that support *ad hoc* data retrieval for reports as in the creation and maintenance of periodic and on demand reports. The tools shall be highly interactive and preferably Web-based, allowing the user to see representative output from the report during its build procedure.

The reporting software shall have full read-only access to the IS&R database and shall support sorting, filtering, algebraic, logical, and arithmetic functions, such as spreadsheet calculations, to allow for report creations. The software provided shall be a commercially available package capable of generating complex reports.

The IS&R shall provide the capability of users to configure report formats. The administrator shall be able to select version control of report definitions to be integrated with the TDMS source control system on a report-by-report basis. Any report may be displayed on the screen, sent to any printer, exported, or sent through an industry standard messaging system (e.g., e-mail) to any destination.

19.1.9.1 Report Generation

Any authorized TDMS user shall be able to schedule the generation of IS&R reports by time and date or on demand. In addition, the user shall have the capability to specify conditions detected by the TDMS such that designated reports are automatically initiated. Reports shall have the capability of being regenerated if a value in the report is adjusted and all dependent values are re-calculated.

The report generation facility shall be able to securely publish these reports in any format (including HTML, XML, PDF, delimited text, Postscript, and RTF) to any destination (including e-mail, Web browser, and file system). The user shall be able to designate the format and destination to which reports are generated. If the destination is a hard copy printing device, the TDMS shall use available (i.e., base operating system) print file-spooling logic. This shall include automatic redirection to a compatible output device and redirection notification to the TDMS administrator and user. The report shall not have to be rebuilt to send it to additional destinations. The IS&R shall track successful report distribution and receipt and shall generate a notification for any delivery failure.

19.1.9.2 Ad Hoc Reporting Feature

The IS&R database tools shall include a method for extracting data using industry standard SQL or ODBC. The TDMS, however, shall allow a less sophisticated user to construct database queries more simply. In this respect, the Authority prefers a tool such as Query by Example (QBE) to be made available.

The simple query tool provided by the Contractor may generate complex SQL. Consequently, it is desirable that the simple query tool shall optionally display the SQL that it generates, so that the more sophisticated user can then view and edit the SQL as required to execute the query.

19.1.10 Historical Power System Views

The TDMS shall have the capability to create views of the state of the power system at given points in the past. These views require not only snapshots of the power system's telemetered and derived measurements and status values, but also the results of various application programs (e.g., State Estimation) along with prevailing alarms as well as snapshots of displays, etc.

Historical views shall be used to support control room activities in the current day and hour operating timeframe. The IS&R shall record such views in a manner that can be accessed quickly for these activities.

Historical views of the power system are required, for example, to support the following processes:

1) Historical data required by the Authority to support business process and decision support. For example, various forecasting activities are based on past history.

2) Disturbance analysis by the Authority to analyze and report on power system events defined by operating policy.

3) Creating scenarios for the Operations Training Simulator.

4) Power system network analysis studies.

19.1.11 Audit Trail

An audit trail of all changes made to the IS&R database shall be maintained and made available for display and printout. 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 of the party making the change. The audit

trail shall include the before and after values of all content changes. Printouts and displays of the audit trail shall be available in formats sorted by:

1) Period (from date/time to date/time)

2) Data identifiers (table/record, value name, substation, field device interface, etc.)

3) User ID.

19.1.12 Web Services

The IS&R function shall support the Web services that will be required by authorized users having access from the Corporate WAN to the Web server in the TDMS DMZ. As specified elsewhere in these Technical Specifications (refer to Clause 15.4.6), this shall be possible by using their workstation browsers, which may be any standard browser such as Internet Explorer. The Web services shall be developed during project implementation based largely on defining the specific data, reports, and displays required by external users on the Corporate WAN. In this respect, displays serving as customized dashboards shall be supported.

19.2 Specific Applications

The TDMS shall support the following specific functions that make use of the general features of IS&R. For related capacity requirements refer to Clause 15 of these Technical Specifications.

19.2.1 Alarm and Event Storage and Retrieval

The alarm and event storage and retrieval function shall consist of a chronological listing of all TDMS alarm and event messages. Each entry in the list shall consist of the same information that is displayed on the TDMS Alarm Summary and Event Summary displays. In contrast to other data stored in the IS&R database, alarms and events shall be stored, but not modified.

Easy-to-use procedures for storing and retrieving the alarm and event messages shall be provided. In addition, the software tools supporting the user with an interest in viewing or analyzing the information shall provide flexible as well as convenient data selection capabilities. In this respect, the facilities to sort, selectively display (filter), and print the contents of the stored alarms and events shall be provided through the IS&R user interface. A user shall be able to select the entries to be displayed or printed based on the following sort and filter parameters and any combinations of these parameters:

1) *Alarms* – Select a set of alarms based on alarm partitioning and severity level.

2) *Events* – Select a subset of events based on user action (including specific users) and application function detected condition (including specific applications).

3) *Substations/Feeders* - Select a subset of alarms or events based on one, several, or all substations/feeders.

4) *Device Types* – Select a subset of alarms or events based on specific device types.

5) *Devices* – Select a subset of alarms or events based on specific devices.

6) *Time Periods* – Select specific time periods of interest.

7) *Text Strings* – Select a subset of alarms or events based on text strings within the messages.

19.2.2 SOE Storage and Retrieval

In a similar manner to alarms and events, IS&R shall result in a chronological listing of SOE data (also refer to Clause 18.1.8). This shall include easy-to-use storage and retrieval procedures as well as flexible and convenient means to sort and search and selectively display and print the contents of the listed data via the IS&R user interface. A user shall be able to select the data to be displayed based on the following sort and search parameters, including any combination of these parameters:

1) *Substations/Feeders* – Select a subset of data based on one, several, or all substations/feeders.

2) *Device Types* – Select a subset of data based on one, several, or all device types.

3) *Devices* – Select a subset of data based on one, several, or all devices.

4) *Time Periods* – Select specific time periods or relative time periods of interest (e.g., twelve hours prior to the current time).

19.2.3 Periodic Data Recording

Using the IS&R, it shall be possible to capture any TDMS database point, such as a manually entered, telemetered, or calculated real-time value, and store this data periodically in pre-defined sets of associated data referred to herein as accounts. Some of the accounts to be captured, the capture periodicity, and the retention period are presented in Clause 15. For each account, the periodicity of storage shall be set independently over a range from 2 seconds to daily. The applicable increments shall depend on the periodicity of storage as follows:

1) For periodicities less than one (1) hour – 1 second.

2) For periodicities of one (1) hour or greater – 1 minute.

The time of the initial data capture shall be set relative to the start of the hour to a resolution of 1 second. For example, it shall be possible to schedule an hourly capture to begin 15 seconds after the start of each hour. Data captures shall be scheduled in absolute clock time, not relative to the completion of each capture, i.e., a data capture schedule for a periodicity of one (1) hour beginning at XX:00:00 shall occur at the start of each hour regardless of the time needed to perform each capture.

Periodic data storage shall include a programmatic interface to initiate and suspend periodic data capture. The interface shall facilitate initiation of single non-periodic (“on-demand”) executions of the data capture process for either one or more of the pre-defined accounts.

19.2.4 Continuous Data Recording

The IS&R shall maintain a continuous record of power system operations by storing selected real-time data including all associated quality codes and supervisory control tags. In effect, the stored data shall represent a sequence of snapshots, each snapshot corresponding to a subset of the real-time conditions that prevailed at the time the snapshot was taken. The snapshots shall not be modified in any way.

Storage optimization techniques shall be applied, e.g., in addition to the possibility of storing snapshots containing all data of interest, it is expected that the stored snapshots shall normally contain only the data that has changed significantly from the previous snapshot.

The user shall be able to retrieve any snapshot by specifying the date and time of interest assuming, of course, that the data recording function was active at that time. Typically, the snapshot shall include status, analog, alarm, and event type data. Data shall be accessible to system operations and Corporate users per their assigned privileges.

Procedures shall be provided for selecting and sorting the recorded data by time and variable and by a combination of these parameters. In addition, tools allowing the selected and sorted data to be used for calculations, video trends, displays, and reports shall be provided.

19.2.5 Historical Playback

The IS&R shall support an historical playback feature, which shall be available to multiple users simultaneously and independently. Each user shall be able to select a start date and time from a disturbance file or the historical alarm and event file or nominate a start date and time. The TDMS shall display the historical values and alarms on the displays that are normally used for displaying real-time data. These shall include the Alarm Summary and Event Summary displays.

The user shall be able to move forward and backward through a set of control buttons on a console, or through the disturbance file or historical alarm and event file, and the corresponding values and alarms shall be shown on the displays as they occurred at that time. In addition, the user shall be able to put the displays into fast forward or backward mode to replay the history at a user nominated rate.

To differentiate execution of the playback function from other functions, an indicator shall appear on each display that is in historical playback mode. The indicator shall always be visible.

Operator actions related to historical playback shall not be processed as events.

The Contractor shall have described all capabilities and features of the proposed playback function in the Contractor’s proposal.

19.3 Prefered IS&R Technology

The Authority’s preferred technology for IS&R implementation is one that is based on a Data Historian solution rather than a Relational Data Dase (RDB) solution. In this respect, the Data Historian software shall be specifically designed to support fault-tolerant as well as high-speed, high-capacity, process data storage and retrieval. It shall be capable of execution on a variety of different OEM servers, support

replication across the Authority's two data centers, and exhibit linear and highly scalable data expansion capabililties without losing its high-speed performance characteristics.

20. Power System Applications

The TDMS shall include HV/MV power system applications that can be used in real-time, study, and simulation modes to support power system operations, planning, and training. This clause of the Technical Specifications presents the minimum functional requirements associated with these applications.

The Dispatcher shall use the Contractor-provided applications executing on the TDMS data center servers to monitor and control both the HV and MV elements of the Authority's power system network within the Dispatcher's assigned AORs. To the extent possible, the requirements herein shall be met by the Contractor's standard (off-the-shelf) EMS/DMS applications and, in this respect, the Contractor's proposal shall have identified which of the Authority's requirements, if any, are not met by these standard applications. The Contractor's proposal shall have also identified any applications and/or any capabilities and features (over and above those specified) that may come with the Contractor's standard EMS/DMS applications as already built-in and available for Authority utilization or activation at no additional cost. In addition, the proposal shall have identified if any such applications may be purchased as options.

20.1 Design Features

It is recognized that EMS and DMS applications have traditionally been designed and executed separately because of the different characteristics of the EHV/HV and MV power system networks to which they relate.

For example, EMS applications relate to EHV/HV power system networks that are generally meshed and typically treated as balanced three-phase networks, whereas DMS applications relate to MV power system networks that are generally open-loop (i.e., radial) and correctly treated as unbalanced three-phase networks that may also include two-phase and single-phase circuits.

Another important difference is that EHV/HV networks are normally associated with sufficient telemetered data (i.e., power system measurements) that enables them to be fully observable by the EMS State Estimation (SE) application without significant dependence on pseudo (i.e., non-telemetered) data, whereas the MV networks are not and, as such, are highly dependent on data that is less accurate and may be derived, for example, from historical load profiles. Within this context, observability means that a feasible solution is possible.

Consequently, in keeping with the traditional approach, the EMS and DMS network analysis applications are specified in these Technical Specifications separately and, in this respect, shall execute in parallel to serve the Authority's overall power system operational needs. On the other hand, where alternative consolidated solutions are available, the Contractor's proposal shall have provided relevant details for Authority consideration. For example, it is conceivable that a single Power Flow function could execute for the entire HV/MV power system network modelled everywhere as a single unbalanced three-phase network.

Within this context, whereas the HV applications may be based on balanced three-phase models of the HV network, the MV applications must be based on unbalanced three-phase models of the MV network. Further, under any conditions that are common to the HV network and any or all MV feeders that the HV network serves (for example, under conditions that correspond to a common instant of time), the HV and MV network solutions must be consistent, i.e., the voltages and currents at their points of interconnection must be the same.

As another important feature of the HV/MV applications, it is required that they can be executed in situations where the power system network may be separated into multiple operational islands, i.e., provided all necessary data is available, the applications shall be able to provide a solution for each island.

20.2 HV/MV Applications

The HV and MV applications shall be fully integrated for efficient execution on the TDMS main platforms. They are listed as follows:

1) Network Topology
2) Dynamic Network Coloring
3) Load Forecast
4) Generation Forecast
5) State Estimation
6) Contingency Analysis
7) Power Flow
8) Fault Level Analysis
9) Open Conductor Fault Detection
10) Fault Location, Isolation, and System Restoration
11) Optimal Feeder Reconfiguration
12) Integrated Volt/Var Control

20.3 Operating Modes

The TDMS shall support three application operating modes, namely, the real-time, study, and simulation modes, where the following definitions apply:

1) *Real-Time Mode* – This is a mode in which an application performs its function by using real-time data and producing information immediately applicable to real-time operations. For example, when triggered by an actual feeder fault, the Fault Location, Isolation, and System

Restoration (FLISR) application makes use of current real-time data to determine the action that should be taken to alleviate the situation. Also, State Estimation uses whatever real-time data is available to produce the equivalent of a power flow solution that represents a "best" estimate of the current real-time state of the power system.

2) *Study Mode* – This is a mode in which an application uses modified real-time or saved data to produce information that can be used to examine alternative hypothetical or postulated operating scenarios. For example, Load Forecast (though it may use real-time load data to make forecast adjustments) does not execute to compute current power system loads, but to predict future power system loads. In addition, as another example, Power Flow can be used to study what happens when changes are made to a power system that is not representative of the current power system state, but of some other postulated state.

3) *Simulation Mode* – In this case, an application runs in an environment where the required real-time and/or saved data is replaced by simulated data. A "dynamic" model of the power system is used to produce the simulated data as the model responds to hypothetical scenarios consisting of time-dependent loads and contrived system events such as feeder faults.

Which of the applications shall execute in one or more of these modes is summarized in Exhibit 20-1. The exhibit also includes SCADA, Load Shedding and Restoration, and SMS as described in Clause 18 of these Technical Specifications.

Exhibit 20-1: Application Operating Modes

MV Application/Function	Real-Time	Study	Simulation
SCADA	X	-	X
Load Shedding and Restoration	X	-	X
Switching Management System	X	X	X
Network Topology	X	X	X
Dynamic Network Coloring	X	X	X
Load Forecast	X	X	-
Generation Forecast	X	X	-
State Estimation	X	-	X
Contingency Analysis	X	X	X
Power Flow	-	X	X
Fault Level Analysis	-	X	X
Open Conductor Fault Detection	X	-	X
Fault Location, Isolation and System Restoration	X	-	X
Integrated Volt/Var Control	X	X	X

20.4 Network Operations Model

Each TDMS main platform shall include a Network Operations Model (NOM) along with the database management tools required to create and maintain this model. The NOM on each platform shall be a synchronized replica of the NOM on the other platform. Within this context, NOM shall serve as a single centralized resource for the HV/MV power system applications and displays. It shall include detailed information concerning the elements of the Authority's HV/MV power system network including their characteristics and connectivity.

Within this context, NOM as a minimum shall include the following capabilities and features:

1) Analytic models of electrically connected elements of the Authority's power system network. These models shall include the EGAT and SPP/VSPP generating units that represent points of power injection into both the HV and MV networks and the loads that are fed mostly by the Authority's MV feeders and their distribution transformers.

2) Ability to accommodate lightly meshed and radial power system configurations including single-phase and two-phase circuits and associated loads as well as non-symmetrical three-phase circuits and loads. In this respect, the models shall allow for three-phase balanced and unbalanced operations.

3) Information for schematic displays of the electrical facilities, showing individual elements and interconnections, along with the operating state and other related information.

4) Information for geographically oriented displays of the distribution network showing the individual elements, their operating state, associated land based information, operations data, facilities, equipment, locations of field crews, and other related information.

5) Operations data such as feeder and device status indications, associated statistics, tags, operating limits, set points, power flows, voltages, currents, transformer tap positions, quality codes, alarms, and outage locations.

6) Facility and equipment information such as status, alarms, location and site details, electrical and mechanical design parameters, photographs, contact replacement indices, operating instructions, and maintenance procedures. This information shall be made available by equipment point and click operations on relevant displays and presentation of a drop-down menu allowing the Dispatcher to select the information of interest.

7) Modeling information for electrical devices and loads. This shall include the ability to represent power system elements such as generators, substation buses, on-load tap changing transformers, reactors, breakers, reclosers, overhead lines, underground cables, voltage regulators, var controllers, load break switches, fuses, switched capacitor banks, distribution transformers, loads (with parameterized voltage dependencies), and automatic transfer switches. Generation modeling shall take unit capability curves into consideration.

8) Modeling that accounts for temporary jumpers, grounds, and cuts. Using a world map display, for example, the Dispatcher shall be able to make changes that are planned (e.g., a lineman

doing maintenance work) and unplanned (e.g., a tree falling and breaking a power line). This feature shall allow the Dispatcher to change the power system model very easily and, at the same time, have the display symbolically updated to show, for example, a feeder being jumpered (attached) to another feeder, grounded, or cut. It shall be possible to "back out" (undo) the change when the repair is completed to restore the power system display and model to their prior states. This feature shall support single-phase as well as three-phase changes, and all such changes shall be made without the need for a formal editing session to modify the TDMS database.

9) Field crew information such as names, planned assignments, completed assignments, and current location.

10) Land based information such as street maps, buildings, waterways, and other landmark details.

20.5 Dynamic Operations Model

The Dynamic Operations Model (DOM) shall be an extension of NOM to support the execution of TDMS applications in simulation mode, i.e., as part of the Operations Simulator (OPS) function described elsewhere in these Technical Specifications (refer to Clause 20.23).

20.6 Network Topology

The power system applications shall include a Network Topology (NT) function. This function shall be capable of automatically analyzing the open/closed status of power system switching devices to determine the electrical connectivity and the energization, de-energization, or grounded status of power system components such as generators, transformers, lines, and capacitor banks.

The status of the switching devices shall be obtained from real-time or manually entered data (also refer to Clause 18.3.2 of these Technical Specifications). These devices shall include all relevant power system elements such as circuit breakers, switch disconnectors, automatic transfer switches, line reclosers, remote controlled switches, and capacitor bank switches. They shall also account for the connectivity changes that occur when temporary jumpers, grounds, and cuts are applied to the power system.

Network Topology shall result in an updated power system model that can be used by the applications which depend on the model to analyze the system under current or postulated system conditions. For example, Network Topology shall automatically and efficiently update the power system model whenever a switching device status change is detected. The user shall also be able to execute Network Topology on demand.

20.7 Dynamic Network Coloring

Dynamic Network Coloring (DNC) shall enable Dispatchers to quickly recognize the power system’s operating status on all associated tabular as well as geographical and schematic displays. As a minimum, this shall allow the energized, de-energized, faulted, grounded, and overloaded conditions of the power system to be differentiated, using color codes or other means, automatically following execution of network applications such as State Estimation.

In addition, Dynamic Network Coloring shall allow users to request distinctive color-coded traces that can quickly highlight electrically connected elements of the power system through simple point-and-click operations. User-requested tracing results shall be displayed only at the workstation where the request is issued; multiple users at different workstations shall be able to request and view different tracing actions in parallel. Such tracing shall include, but shall not be limited to:

1) Highlighting the entire electrical island or feeder section to which a power system device selected by the user is connected.

2) Highlighting the upstream power supply path from the user-selected device to the head-end power injection point including the path's load break switches, reclosers, and circuit breakers.

3) Highlighting all feeder sections downstream of the user-selected device.

20.8 Load Forecast

To support operations planning and analysis, Load Forecast shall execute on demand to forecast 15-minute area loads for up to fifteen (15) days in the future. These loads shall correspond to the HV and MV loads served by the power system network within all or any of the Authority's 12 service areas.

The user shall be able to save any of the load forecasts as a save case. Save cases shall be for up to seven (7) days past, present, or future. The user shall be able to save any load forecast for the next seven days following the current day and designate it as the active forecast to serve as the "official" load forecast governing the current operational plan. The active forecast will be updated at least once per day.

It shall be possible to use any of the saved load forecasts, together with relevant load distribution factors, to establish individual feeder loads required, for example, to support execution of the Power Flow application in accordance with a Dispatcher entered date and time. Also refer to Clause 20.9.

The user shall be able to make manual adjustments to any of the saved forecasts. In addition, with respect to the active forecast, Load Forecast shall make future half-hourly forecast adjustments automatically. This shall be based on the amount of mismatch between the forecasted loads and the actual loads of previous half-hours as they become known.

As parameters used by the Load Forecast application, the user shall be able to enter up to seven (7) user-defined weather conditions for up to three (3) predefined times of the forecast day. These conditions may include temperature, barometric pressure, relative humidity, precipitation level, wind speed, wind direction, and luminosity. Multi-day forecasts shall be constructed by permitting the user to define the input data for each day within the maximum study period.

A similar day forecast may be used. This shall be based on load curves representing the daily 15-minute loads that occurred in the past for each of fifteen (15) different day types. Provision shall be made for storing these load curves for the last 25 months. The storage shall be updated each day by using the most current actual load curve to effectively replace, on a "first-in, first out" basis, the oldest load curve of the same day type.

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. 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. The user shall be able to modify any of the forecast's loads manually. In addition, the user shall be able to scale the entire forecast by simply specifying an appropriate peak load value.

The user shall be able to print and display the forecasts on a territory wide and Authority area-by-area basis in both tabular and graphical form. This shall include the ability to display the active forecast with the actual loads of current and past days superimposed.

As an alternative to the similar day forecast, methods that utilize weather-adaptive and neural network techniques are also acceptable.

20.9 Bus Load Forecast

To support the power system applications, the Bus Load Forecast (BLF) function shall be in accord with the Load Forecast function with respect to time intervals (minutes, hours, days) and day types and shall provide the capability to calculate bus real and reactive loads based on characteristics dependent on current, past, and future states of the power system. This shall include the capability to:

1) Utilize load profile characteristics derived from data available from the TDMS Historian.

2) Forecast the real and reactive load-to-voltage dependencies for two modes of operation:

    a) Normal operating conditions (linear dependencies can be used).

    b) Emergency operating conditions (second power polynomial dependencies).

3) Adapt bus load values based on characteristics associated with:

    a) Substation reactive devices.

    b) OLTC transformers.

    c) Mvar reserves under normal and emergency voltage limits.

    d) Bus voltage limits.

    e) P-Q load curves for SPP and VSPP generation units.

In addition, the Bus Load Forecast function shall provide the capability to generate a forecast for load groups and their associated characteristics. A load group can contain more than 1 (one) bus or more than 1 (one) substation. Load groups shall correspond to those defined for use by the applicable power system applications such as the State Estimation function.

20.10 Distribution Load Allocation

The Distribution Load Allocation (DLA) function shall serve as a source of real-time pseudo-measurements and forecast (future) values corresponding to distribution transformer loads (both active and reactive). Thus, DLA shall provide estimates of distribution transformer loads that can be used, for example, as preliminary input to the MV State Estimation (SE) function or as forecasts serving as preliminary input to DMS study functions such as Power Flow (PF), Integrated Volt-Var Control (VVC), and Optimal Feeder Reconfiguration (OFR).

The basis for estimation initially shall be past distribution transformer loads categorized, for example, by month, day-type, and (where available) the day-type's prevailing weather conditions These load profiles shall be derived from Authority historical records of individual customer loads served by each distribution transformer.

Otherwise, once the TDMS enters commercial operation, the capability to maintain load profiles automatically shall be supported. This shall be accomplished by periodically importing the latest customer loads on each distribution transformer via the required TDMS interface with Authority AMI facilities. The capability to incorporate weather data shall also be provided. Within this context, details on how the distribution transformer loads can be updated over time shall be resolved during project implementation.

The capability to automatically adjust the loads according to their known or assumed correlation with the total power system load established by the Load Forecast (LF) function shall be provided.

The DLA user interface shall include the capability of the user to visualize the distribution transformer load profiles as time-based curves on displays that may cover one or more user-specified days. The following DLA capabilities shall also be provided:

1) Manual load adjustments.

2) Automatic provision of the distribution transformer loads as and when required by the MV network's SE function.

3) Provision of the distribution transformer loads as required to support MV network studies based on the date and time that the user specifies.

20.11 Generation Forecast

The intent of the Generation Forecast (GF) function is to provide forecasts corresponding to the individual and total real and reactive power outputs from VSPP and SPP distributed generation resources such as Solar-PV and wind-turbine renewable energy plant. The power output values shall be capable of being used to support operations planning and analysis as well as the Power System Applications.

GF shall forecast power output values by accounting for the statistical dependency of distributed generation on weather data such as intermittent solar irradiation, cloud cover, and wind speed statistics on a zone-by-zone and/or voltage connection level basis throughout the Authority's service territory.

The zones shall be based on those that statistically are exposed to similar weather patterns. GF shall also consider any available information that may be known about the nominal and/or current capacity of the plant and their status, such as their expected output during the generation forecast period. In this respect, the capability to use any applicable information derived from the Authority's future Demand Response (DR) system shall be supported as well as any relevant information maintained by the Equipment Outage System (refer to Clause 18.4).

Within this context, key functional requirements include:

1) Capability to forecast individual and total distributed generation output on demand at 15-minute intervals covering periods from 1 (one) hour ahead to 1 (day) ahead.
2) Capability to generate the historical data it needs for statistical sampling and reference and for tuning the generation forecast model through a learning process.
3) Use of an adaptive statistical forecast model to compute distributed generation forecasts from inputs such as weather conditions, generation plant type, nominal or current rating, and online/offline status.
4) Ability of user to modify the forecast by entering data for any time slot.
5) Capability of comparing the forecast result with any actual distributed generation output (as may be known) by trending, for example, on an interval of 15 minutes.
6) Capability of GF to continuously update itself over time. Provision shall be provided for the user to initiate a learning process by considering the forecasts as well as the actual forecasts and weather information.
7) Capability of the adaptive model to be tuned easily by modifying the appropriate parameters of the model.
8) Capability to display GF results on an Authority territory-wide, area-by-area, and zone-by-zone basis.

20.12 State Estimation

State Estimation shall provide a complete and consistent power flow solution of the HV/MV power system that best fits all available power system SCADA measurements and/or pseudo-measurements associated with the relevant NOM, which for the MV network shall be based on an unbalanced three-phase model. It shall execute on demand, periodically (initially every 15 minutes), and when triggered by a power system event that creates a change in network topology.

20.12.1 Measurement Set

The State Estimation measurement set shall include all valid (acceptable) data representing the real-time measurements or pseudo-measurements that correspond to the time and date of interest.

The pseudo-measurements, used where actual measurements are insufficient to obtain a feasible solution, may include calculated data points from SCADA and estimated loads and status values derived automatically by the State Estimation application and/or other TDMS functions. Non-valid

data, i.e., data deemed to be of unacceptable quality shall be discarded until it is otherwise considered valid.

As a minimum, the measurement set used by State Estimation shall include:

1) MW and MVAr flows.

2) MW and MVAr sources of power and loads.

3) Bus voltages.

4) OLTC tap positions.

5) Switch and breaker status values.

20.12.2 Required Characteristics

State Estimation shall include, but shall not be limited to the following characteristics:

1) Electrical islanding shall be resolved such that the solutions from all such islands shall be integrated into a single power system solution.

2) Measurement set data shall be assigned weighting factors associated with the relative accuracy of the measurements. For example, valid SCADA measurements shall be assumed to be of higher accuracy than pre-defined load profile values used as pseudo measurements.

3) If available, properly time-aligned synchrophasor measurements shall be capable of being used.

4) Bus injection pseudo-measurements shall be estimated using techniques such as those that depend on load distribution factors. These factors shall adapt to load patterns that change over time using adjustable exponential smoothing parameters.

5) To account for multiple voltage measurements at a bus, their assigned weighting factors shall be considered.

6) Bad data shall be detected provided sufficient measurement redundancy exists. Data determined to be bad shall be assigned a bad-data quality code and rejected for use until the quality code is removed.

7) Input data quality codes shall be considered. If bad data is indicated, this data shall also be rejected.

8) Bus voltages shall be maintained between high and low limits on regulated buses.

9) Where necessary, tap positions shall be estimated.

10) Where necessary, the switch positions of switched capacitor banks and var controllers shall be estimated.

11) Line and transformer overload, voltage, and power factor violations shall be detected.

12) The user shall be allowed to adjust State Estimation control parameters such as convergence tolerance and maximum number of iterations.

20.12.3 Output

The State Estimation solution shall be made available to the user in both one-line diagram and tabular display formats, any or all of which shall be capable of being printed. In addition, the user shall be able to save the solution as a saved base case, so that it can be used as a starting point for study applications such as Power Flow. For the number of "save cases" required, refer to **ผิดพลาด! ไม่พบแหล่งการอ้างอิง**. SE solutions shall be capable of being printed and exported in flat file formats such as "cv" and "xml."

If violations such as overloads or over/under voltage levels are detected, the violating values shall be displayed as values in alarm. All bad data shall be displayed with the appropriate quality code, and summary displays showing all bad data shall be provided.

SE save cases shall be stored in auxiliary memory. It shall also be possible to archive save cases.

20.13 Power Flow

The Power Flow (PF) application shall calculate the state of the Authority's HV/MV power system network based on:

1) Real-time and/or saved base case data.

2) Manually-entered input.

3) Models corresponding to the operation of automatic devices such as OLTC transformers, voltage regulators, capacitor banks, and var controllers.

4) Models of power plant connected at HV and MV network levels.

5) Models of distributed generation (e.g., small-scale Diesel, Solar-PV, and Wind-Turbine units) as well as loads along the feeders.

For the Authority's MV feeder network, PF solutions shall be based explicitly on unbalanced three-phase network models. For the HV networks, they may be based on balanced three-phase models. On this basis, it shall be used on demand to execute power system studies that may include the entire HV/MV network or portions of the network in accordance with a control center's areas of responsibility. For example, the Dispatcher shall be able to execute the PF application on demand for any number of feeders associated with a substation selected via a schematic or geographical overview display and see the results on the same display.

The studies shall be performed starting from a base case, such as the base case that corresponds to the current State Estimation solution or to a previous State Estimation or PF solution, referred to herein as a "save case." Prior to execution, the Dispatcher shall initiate the base case changes to define the power

system ("what if") conditions that need to be studied. Thus, DPF users shall be able to modify power system connectivity (e.g., by opening or closing switches), adjust real and reactive power injections such as feeder loads, increase or decrease generator voltages, change transformer tap positions, etc.

20.13.1 Required Characteristics

The PF application shall include, but shall not be limited to the following characteristics:

1) At user option, the discrete tap positions of OLTCs and line voltage regulators shall be automatically adjusted to maintain specified voltages while complying with prescribed tap position limits.

2) Capacitive line charging effects shall be modeled, including the insulation losses of underground cables where applicable.

3) Switched capacitor banks shall be modeled to account for their var control capabilities. Automatic switching shall be enabled or disabled, as determined by the user or by associated local/remote control status points.

4) Var controllers shall be modeled where these independently acting devices are used to support voltages and power factors.

5) Starting from a base case, loads shall be adjustable on an individual basis. In addition, they shall be capable of being initialized using load distribution factors derived from State Estimation results and historical records. The load distribution factors shall correlate loads at individual buses with variables such as system, substation, and feeder loads as well as date and time. Correlation based on feeder loads that are assumed proportional to the rating of their distribution transformers shall also be possible. Subsequently, initialization of the loads in study mode shall depend on the date and time that applies to the study and any user modifications to the system, substation, feeder, and/or individual loads.

6) Loads that depend on voltage shall be modeled using separate expressions for real and reactive power. In such cases, the loads shall be adjusted to account for the changes in voltage that occur during the iterative power flow solution process.

7) Transformers shall be modeled by explicitly considering copper losses, core losses, and voltage dependence.

8) Generators, including external EGAT and internal small power producer (SPP) units, shall be modeled as either constant real and reactive power devices or as constant power (i.e., real power) and voltage devices. These models shall take into consideration relevant capability curves.

9) Models of renewable energy resources such as the Solar-PV and wind-turbine plant of SPPs and VSPPs shall be supported.

20.13.2 User Input

PF shall be designed so that a minimum amount of user input is required. This input shall largely be limited to identifying the base case for the study and then making all desired changes prior to execution. Line outage, re-sectionalizing, or other configuration studies shall simply require the user to change the status of the appropriate switching devices on the associated one-line display. Other changes shall only require simple numerical entries and, where appropriate, the selection of any relevant solution option available.

Input shall include the capability to adjust the algorithm's control parameters such as convergence tolerance and maximum number of iterations.

The user shall be able to execute power flow studies for a particular circuit, a particular substation, or a particular section of the power system (such as the power system section covered by two or more substations) using current base case or postulated load conditions.

Multiple independent users at different workstations shall be able to execute the PF application simultaneously and independently, each starting from their last execution or from a selected save case. In these "what if" studies, alarms generated by PF shall not be treated as real-time alarms, but shall be retained for display at the workstation on which the PF application was run. In modifying the base case prior to execution, the user shall be able to scale loads, specify loads individually, modify bus voltages, apply temporary changes such as cuts, jumpers, and grounds, and change device status values.

20.13.3 Output

As a minimum, the PF application shall calculate the following quantities:

1) Real power, reactive power, and three-phase current for all circuit elements.

2) All three phase-voltages at all buses, including the LV side of distribution transformers.

3) Total real and reactive losses, line losses (load and no load), and transformer losses (load and no load) both in kW and in percent.

4) Tap positions for substation transformers and line voltage regulators.

5) Switch positions for capacitors and automatic transfer switches.

6) Feeder voltage drops.

7) Phase imbalance of the unbalanced 3-phase circuits (e.g., average phase current minus minimum phase current, divided by the average current).

8) Voltage imbalance of the unbalanced 3-phase buses (e.g., maximum voltage minus average voltage, divided by the average voltage).

9) Voltages and currents on single and two-phase portions of the network.

The power flow results shall be made available in tabular form and on one-line diagrams equivalent, for example, to the graphical displays used for real-time dispatching. In addition, the results shall be subject to the same limit alarm processing as other calculated data, i.e., each calculated variable shall be tested against three pairs of alarm limits, and an alarm shall be generated when a limit violation is detected. Alarms and overloads determined by PF shall be indicated to the user simply and clearly. All line sections that are overloaded and all buses that have voltage violations shall be highlighted in color when the user selects the appropriate display mode.

As for State Estimation, the TDMS shall provide the user with the capability to print any selected PF tabular or graphical display and to store and retrieve PF solutions as save cases. For the number of "save cases" required, refer to Exhibit 15-8. PF solutions shall be capable of being printed and exported in flat file formats such as "cv" and "xml."

20.14 Contingency Analysis

The Contractor shall provide a Contingency Analysis (CA) application that shall be used to assess the security of the Authority's HV power system under specified contingency conditions. It shall consist of:

1) Contingency definition.

2) Contingency screening.

3) Full contingency analysis.

Contingency Analysis shall use the latest State Estimation solution for real-time security assessment of the power system. In this respect, the user shall be able to have CA run automatically following each SE solution. Furthermore, CA shall be able to use a saved Power Flow solution for assessing power system security in study mode. Contingencies shall be applied to either of these solutions serving as the CA base case. Each contingency may consist of single or multiple outages of power system components. Power flow solutions shall be used to analyze the effects of these contingencies.

Contingency Analysis shall provide the capability to evaluate a contingency involving increase or loss of generation or increase or loss of load by generation reallocation in the external network. Generating unit limits shall not be violated by generation reallocation. In this respect, CA shall apply the same unit limits as used by the other Power System Analysis functions.

The CA function shall include the capability to define, edit, validate, and maintain contingency cases for real-time and study. In this respect, it shall have two components involving: (a) a base contingency case definition process and (b) a dynamic contingency case re-definition process.

20.14.1 Contingency Definition

It shall be possible to define contingencies as a combination of outages and/or the placing in service of one or more power system elements. This may include the opening or closing of one or more associated switching devices. The user shall be able to modify contingencies via user interface displays.

It shall be possible to organize the contingencies into groups. A contingency may be assigned to any number of groups and the assignments can be modified interactively. It shall also be possible for the user to enable/disable any or all contingencies of a group.

In addition, the user shall be able to perform contingency case list updates, as necessary, to reflect equipment additions, deletions, or modifications to power system equipment.

20.14.2 Contingency Screening

A contingency screening capability shall be provided. The goal of contingency screening shall be to identify as quickly as possible the most critical contingencies, thereby reducing the number of contingencies that must be analyzed in full for greater accuracy. The contingency screening function shall be capable of handling contingency cases of any complexity, including cases that cause bus splits. Any contingencies leading to bus splits, isolated equipment, or changes in network islands shall be reported.

Contingency screening shall process the specified list of contingencies and rank the contingencies from the perspective of how severely they violate the power system's reliability criteria. The ranking shall be tunable by using weighting factors. Based on this ranking, a reduced contingency list shall be constructed for Contingency Analysis processing in full.

It shall be possible to specify how many of the highest ranked contingencies shall be analyzed in full. As an alternative, it shall also be possible to specify that all contingencies resulting in violations during the screening process be analyzed fully and completely.

The user shall have the additional ability to specify that certain contingencies or all contingencies be processed in full regardless of the contingency screening's ranking, thereby ensuring that these contingencies will be accurately analyzed. Furthermore, in real-time mode, contingencies that caused a violation in the previous execution of the CA function shall be added to the contingency list requiring more accurate processing.

The Contractor shall tune contingency screening so that any contingency that may result in significant overloads or voltage violations is captured by the screening process. This may be achieved by tuning weighting factors used for contingency ranking, placing contingencies on the reduced contingency list without screening, changing limits used for violation checking, or by changing the selection algorithm itself (e.g., adding an additional iteration). After tuning, performance requirements shall still be satisfied.

20.14.3 Full Security Analysis

Full Contingency Analysis shall be executed automatically after contingency screening. The objective shall be fast yet accurate analysis of the contingencies in the reduced contingency list from the perspective of power flow and bus voltage limit violations. A robust power flow solution shall be used.

It shall be possible to enable or disable power flow controls, such as Mvar limiting for generators, generator voltage control, shunt reactor and capacitor voltage control, and transformer LTC voltage control on a system-wide basis, type basis, or on an individual device basis.

Contingency cases that fail to converge shall be reported. To further investigate non-convergence, it shall be possible to obtain iteration and convergence records for a CA execution as in case of a PF execution.

20.14.4 User Input

User input functions shall be provided to facilitate definition, editing, and validation of contingency cases. The contingency definition and editing shall be made as simple as possible through interactive and menu-driven procedures.

Within this context, the capability shall be provided to pre-define a class of contingencies that by default are automatically created when a new substation is commissioned and modeled as part of the power system's NOM. This shall include, for example, the automatic creation of contingencies that entail loss of substation incoming lines and/or power transformers.

It shall be possible to identify equipment to be included in a contingency by selecting equipment from a one-line diagram as well as from a tabular display. In addition, it shall be possible to enter or edit equipment names.

Through simple interactive procedures it shall be possible to assign or reassign contingencies to groups and specify which groups are included in the real-time or study mode analysis.

20.14.5 Output

The primary output of the CA process shall be provided by the full Contingency Analysis function. Displays shall be provided to show contingencies with their violations. The presentation of these contingencies shall be ordered in accordance with the severity of their associated violations. Within each contingency, the presentation of its individual violations shall also be ordered in accordance with their severity.

For each violation that is presented, pre-contingency and post-contingency values as well as the violated limits shall be displayed.

The user shall be able to distinguish between new violations and violations that have already been detected in the previous execution of the full CA function.

20.15 Fault Level Analysis

The Fault Level Analysis (FLA) application shall be designed to analyze the Authority's HV and MV power system networks such that one or more users may request the execution of independent studies that calculate the voltages and currents due to a postulated fault condition. The function shall include the capability to calculate and compare fault currents against applicable power system limits such as circuit breaker and line recloser ratings.

Fault Level Analysis shall perform these studies starting from a PF or SE solution including corresponding save cases. This feature shall be supported by the ability to also save and retrieve base cases created by the FLA application itself. Prior to executing a study, Fault Level Analysis shall allow

the user to modify the input conditions. In addition to these capabilities, the user shall be able to select and print any of the tabular and graphical displays that correspond to the Fault Level Analysis application.

Selected study conditions shall include phase-to-ground, phase-to-phase, and three-phase faults. The ability of the user to specify bus section faults, feeder section faults, and fault impedance values shall be provided. The user shall also be able to specify a study based on zero pre-fault current (flat voltage) conditions or actual pre-fault current conditions.

Voltages and currents at all system wide buses for each specified fault condition shall be calculated. Results shall be shown on the one-line displays of the power system. Fault currents that exceed acceptable fault-current levels shall be highlighted.

20.16 Open Conductor Fault Detection

Currently, the Authority has no device installed that can detect the presence of open conductor faults directly, so an application referred to herein as the Feeder Open Conductor (FOC) application capable of detecting the presence of open conductor faults on MV feeders shall be provided. Open conductor faults are of special concern with insulated conductors. Insulated conductors that are broken are more likely to be a danger to passersby than other broken conductor types such as bare aluminum conductors. The reason is that people may be tempted to pick them up while still energized.

The Feeder Open Conductor application shall analyze whatever three phase voltage and/or ampere measurements are available from nearby field device interfaces, e.g., FDIs such as SRTUs and FRDCUs, to alert the Dispatcher to open conductor situations.

The detection logic may vary depending on the available data. In this respect, logic based on zero current values in combination with unbalanced voltage and current calculations shall be considered.

Once an open conductor fault is detected, an event message shall be issued to notify the Dispatcher, and the presence of the fault shall be clearly identified on relevant sections of the associated feeder as shown on one-line power system displays.

20.17 Fault Locator

On TDMS detection of a feeder fault based on indications from one or more down-line fault passage indicators, the Fault Locator (FLO) function shall present potential fault locations by using, for example, fault impedance data that may be telemetered from distance relays or by calculating distances to fault using telemetered voltage and fault current values.

The capability to narrow the possible number of fault locations using outage confirmations obtained by the TDMS from customer smart meter pings shall also be provided.

Non-uniform feeder constructions shall be considered, i.e., consideration shall be given to feeder segments that are different in their impedance values.

Where there are multiple fault location possibilities on different branches of the feeder, FLO shall highlight all of them on graphical displays of the feeder.

20.18 Fault Location, Isolation, and System Restoration

The objective of the Fault Location, Isolation, and System Restoration (FLISR) application is to improve customer service by minimizing the duration and extent of forced outages due to real-time faults directly affecting the MV power system network. In this respect, FLISR shall automatically detect the presence of sustained HV/MV substation and MV feeder faults and recommend whatever action is required to isolate such faults. In addition, FLISR shall provide recommendations aimed at restoring service to as much of the affected load as possible. If enabled, FLISR shall be able to implement the recommendations automatically.

Whenever sustained faults are detected by FLISR, the Dispatcher shall be notified by a special FLISR "alarm" indication and, upon acknowledgement, taken directly to that part of a schematic or geographical world-map display where the fault has occurred and where the results of any FLISR actions as well as the fault information reported by FDCU/FRTUs (such as fault current direction) can be viewed. Furthermore, the Dispatcher shall be able to quickly navigate from this display to the display where the FLISR recommendations can be viewed.

20.18.1 General

Detection and confirmation of sustained faults shall make use of telemetered data such as information from fault passage indicators and other sources such as SRTUs and FDCUs associated with substation circuit breakers, substation and feeder line reclosers, and feeder remote controlled switches.

For a sustained HV/MV substation fault (such as HV incoming line or HV/MV transformer faults), FLISR as a minimum shall recommend the most appropriate reconfiguration actions that can quickly restore power to all affected MV feeders by switching to alternative sources of power as may be available. For a sustained fault on an MV feeder beyond the substation fence, FLISR shall also analyze all available telemetered data automatically and, as a minimum, recommend the appropriate actions (such as closing open tie-switches between feeders) that will restore power to as many of the feeder customer loads as quickly as possible.

FLISR's recommended actions shall be generated as a display to the Dispatcher. This display shall include an estimate of the amount of load (pre-fault load) that will be restored should the recommended restoration action be implemented. If the Dispatcher approves the FLISR recommendations, a corresponding SMS switching order shall be automatically generated, and the Dispatcher may then execute the order via the SMS application. In addition, the Dispatcher shall be able to pre-configure FLISR so that it performs some or all appropriate switching without presenting its recommendations.

Once an outage is cleared, FLISR shall recommend the required switching that will return the power system to its pre-fault configuration.

20.18.2 Required Characteristics

The FLISR application shall include the following capabilities and features:

1) Ability to locate any sustained fault as detected, for example, by telemetered fault passage indications.

2) Ability to handle faults occurring on multiple feeders even if at the same time.

3) For an MV feeder fault, ability (if Dispatcher-enabled) to automatically: (a) isolate the fault by opening the closest remotely controllable line reclosers or remote-controlled switches and then (b) restore power to the now healthy upstream feeder sections by reclosing the feeder's circuit breaker or line recloser, i.e., the device that tripped on occurrence of the fault.

4) Once an MV feeder fault has been isolated, ability (if Dispatcher-enabled) to automatically restore power to the now healthy downstream feeder sections by switching them to one or more alternative sources of power, e.g., by closing normally open tie switches between feeders.

5) When not performing automatic switching, ability to present the recommended switching to the Dispatcher, who can then decide to have FLISR implement the recommended switching actions or make use of the SMS facilities to implement them.

6) Ability to have its execution suspended entirely or on a substation-by-substation basis.

7) Ability not to consider switching devices that the Dispatcher has tagged, for one reason or another, as unavailable.

8) Ability to monitor circuit breaker and line recloser operations to discriminate between authorized open commands and unauthorized trip commands. If the tripped breaker has an automatic reclosing relay, but the lockout state is not telemetered, FLISR shall wait for a pre-programmed delay to ensure lockout has occurred.

9) Ability to check the fault indication points from FDIs, fault passage indicators, and protection relays to determine the line section where the fault has occurred. When there are multiple fault indications they shall be checked for consistency. Any inconsistencies shall be reported to the Dispatcher as an alarm and no further analysis or recommendation shall be performed. After locating the faulted section, FLISR shall issue an event message that identifies the faulted feeder section and the faulted section shall be distinctively highlighted on network displays.

10) Ability to present potential feeder fault locations by using, for example, fault impedance data that may be telemetered from distance relays or by calculating distances to fault using telemetered voltage and fault current values. Possible non-uniform feeder construction along its length shall be considered. When there are multiple fault location possibilities on different branches of the feeder, FLISR shall highlight all of them on graphical displays of the feeder.

11) In determining the switching actions that, following fault isolation, can be used to restore power to all healthy downstream feeder sections that are de-energized, ability to determine the "best" feeder reconfiguration, i.e., load restoration, strategy such that:

a) The maximum amount of load is restored while ensuring no overload or voltage violations occur. This shall be checked automatically by appropriate Power Flow (PF) solutions.

b) The Dispatcher shall be able to select which SCADA limits (operating, long term emergency, or short-term emergency) should be used by FLISR. In addition, the Dispatcher shall be able to modify these limits.

c) To maximize load restoration, the disconnected loads may be broken down into segments so that as many of these segments as possible can be transferred to alternative sources of power, i.e., to alternative feeders. This may require the alternative feeders to be reconfigured as well.

12) Ability to determine load restoration actions when more than one feeder at a time is subject to faults. This shall include feeders fed from the same substation and sharing the same alternative feeders as may be available for power restoration.

13) Ability to use breaker trip and relay data derived from SRTUs, for example, to recognize faults within substations including transformer banks or any fault on the primary side of these banks that cause loss of outgoing feeder voltage and current. These faults will normally be cleared by substation protection devices, so FLISR (if necessary) need only determine possible restoration switching, including the closing of secondary bus tie breakers. Otherwise, after a Dispatcher-adjustable time interval, FLISR shall determine the switching actions (such as closing normally open feeder tie switches) that can be used to reconfigure any remaining de-energized feeders so that they are connected to one or more alternative power sources such as other substations and/or feeders. To avoid unnecessary reconfigurations, FLISR shall use more than one substation SCADA point and relevant logic to safeguard against mere failure of a SCADA voltage signal.

14) Ability to estimate and display the total load and load points that are expected to be restored following each recommended control action.

15) Ability to support Dispatcher investigation of alternative restoration strategies prior to execution of a final restoration switching sequence. This shall include modification of FLISR parameters, application or removal of tags on switching devices, followed by a re-execution of FLISR to determine a different recommendation. For example, if the field crew is expected to take a long time to repair the faulted feeder section, the Dispatcher may request the downstream restoration process not to consider switching to restore the unserved pre-fault load, but a load that is higher or lower.

16) In making recommendations, ability to identify any manually operated switches, e.g., ganged air break switches, that are closer to the fault than the remotely controllable switches. Thus, if opening these switches by the field crew would allow more load to be restored, FLISR shall be able to provide the corresponding feeder reconfiguration actions to take.

17) After field crews have repaired a faulted feeder section, ability of the Dispatcher to request FLISR to determine the switching actions to return the network to its pre-fault state. If there were load transfers to adjacent feeders, the Dispatcher shall have the option of returning those loads back to their pre-fault feeder without de-energizing them (close first, then open) or allowing a temporary de-energized state (open first, then close) to avoid potentially dangerous loop flows.

18) When FLISR determines the return to pre-fault condition switching actions, ability to check that none of the switches were operated manually or by a different FLISR fault condition. If so, an alarm shall be issued and the Dispatcher requested to approve the proposed switching or to manually perform alternative switching.

19) If a FLISR load transfer recommendation would cause a line recloser or line/recloser regulator to be "back-fed", ability to issue a special warning message along with the switching action.

20) Ability to support faulted feeders with multiple power sources (such as VSPPs).

20.19 Optimal Feeder Reconfiguration

An Optimal Feeder Reconfiguration (OFR) function shall be provided capable of creating switching plans that transfer segments of MV feeder load to alternative sources of power by changing the status of feeder sectionalizers such as line reclosers, remote controlled switches, and manually operated air-break switches. This includes changes that result in different locations for the normally-open tie-points between feeders.

OFR shall support several problem formulations that define one or more operational objectives related to HV/MV substation transformer and MV feeder segment reconfigurations, including minimizing the number of switching operations, improving reliability, avoiding or reducing overloads and voltage violations, and minimizing power losses. For example, this includes the objective of reducing overloads during peak load conditions within a Dispatcher-defined time window.

OFR shall be enabled in real-time or study mode and shall be activated on-demand or automatically depending on observed or calculated power system conditions. On this basis, it shall provide a set of recommended switching actions such as:

1) Those that optimally unload overloaded feeder segments by reconfiguring the MV network with respect to the feeder segments and their connections to substations. No new overloads on feeders or substation transformers shall be created.

2) Those that optimize the location of normally open points in such a way that the MV network reliability indices will be improved. In this respect, for example, the known frequency of faults on feeder segments and the different number of customers connected to feeder segments shall be considered.

A "Return to Normal" mode shall be provided by means of which OFR shall generate a switching plan that restores all switches to their normal state for a given substation or group of substations with the minimum interruption of supply to customers. The results shall be presented as a set of valid switching plans.

Switching plans generated by the OFR function shall be made available such that the Dispatcher is able to select the most appropriate plan for automatic transfer to a formal switching order, which can then be carried out automatically or step-by-step following the procedures of the SMS function (refer to Clause 18.8).

20.20 Integrated Volt/Var Control

The Contractor shall provide an integrated Volt/Var Control (VVC) application. VVC shall determine the control actions to be taken to achieve more efficient and effective HV and MV network operations. VVC may have two sub-functions called Var Control and Volt Control, which may be activated in combined (integrated) form or independently of each other. Within this context, VVC shall execute periodically as well as on demand.

Possible control actions include:

1) Shunt capacitor bank switching.

2) Adjustments to transformer tap positions, line recloser/regulator tap positions, and line recloser/regulator automatic voltage regulation (AVR) set points.

3) Adjustments to settings corresponding to possible Authority installed devices in the future such as Static Var Compensators (SVCs).

4) Control of Distributed Energy Resources (DERs), including the control of inverters associated with Solar-PV and Wind-Turbine units.

20.20.1 Var Control

The main objective of Var Control is to ensure that power factors at certain specified points in the power system are maintained above acceptable limits while meeting all other applicable power system constraints. These power system points are defined as follows:

1) Power delivery points between the EGAT and Authority power systems.

2) Power supply points at Authority substations and distribution transformers.

3) Points of connection corresponding to DERs and/or SVCs.

To achieve this objective in real-time or study mode, Var Control shall determine a set of recommended on/off control signals that can be used to operate switched capacitor banks, DERs, and/or SVCs. In case of DERs, for example, control shall also be possible by sending signals to those that have smart inverters capable of adjusting DER reactive power settings. Otherwise, in study mode, it shall be possible for Var Control to also consider the hypothetical control of capacitor banks, DERs, and SVCs that are unable to be controlled from the TDMS.

Solutions to the above stated problem may be achieved using one or more objective functions and associated function minimization techniques. For example, the solution may be formulated in either of the following two ways:

1) Determine the control actions that will minimize power system losses while ensuring all power factors of interest are no less than their set target values and all other constraints such as voltages limits and equipment ratings are not violated. In this formulation, the power factors are treated as constraints, i.e., they are not treated directly as objective function variables.

2) Determine the control actions that will minimize power factor penalty functions while meeting all other power system constraints. In this formulation, by assigning penalty functions to the power factors, the penalty factors are treated directly as objective function variables, the penalty functions only being effective if the power factors are below their targeted values.

Other formulations shall also be possible. The general nature of these formulations is further illustrated in Clause 20.20.3 below.

20.20.2 Volt Control

The objective of Volt Control is to try to reduce MW load demand in such a way that this demand is below limits set by the Dispatcher. This may be necessary, under peak load conditions, to avoid the possibility of having to shed load if power from EGAT becomes restricted. Such functionality is typically referred to as Conservation Voltage Reduction (CVR).

To achieve this objective, the Dispatcher shall be able to use Volt Control on an individual feeder or substation basis. Thus, Volt Control shall issue control signals to OLTC transformers and voltage set points to AVR devices to reduce voltage profiles across feeders and thereby achieve reductions in corresponding load demands. The impact of these control actions, however, shall be limited to prevent violation of the Authority's minimum voltage requirement on the secondary of MV/LV distribution transformers.

When Volt Control is not activated, the Authority intends to continue using the hardware-based AVRs that exist on substation transformers and line recloser/regulators. Consequently, when Volt Control is activated, the hardware-based AVRs must be turned off (i.e., set to manual). Otherwise, these devices would tend to counter the voltage reduction effort.

20.20.3 Integrated Optimal Control

In general, VVC shall implement the Var Control and Volt Control sub-functions in the form of an integrated optimization problem having, as a minimum, the following objective functions, controls, and constraints to choose from:

1) **Objective Functions**

   a) Minimization of MW losses.

   b) Minimization of power factor penalty functions.

   c) Minimization of total MW demand (energy conservation).

   d) Minimization of total Mvar demand (emergency var support).

2) **Controls**

a) Var Control Active

i) Switched capacitor banks in substations, typically three capacitor banks in parallel where each bank may be switched on or off independently.

ii) Switched capacitor banks on feeders, typically a single capacitor bank that may be switched on or off remotely.

iii) DERs and SVCs at HV and MV points of connection.

b) Volt Control Active

i) Transformer tap positions and/or their AVR voltage set points.

ii) Line recloser/regulator tap positions and/or their AVR voltage set points.

3) **Constraints**

a) Var Control and/or Volt Control Active.

i) Maximum and minimum limits on voltage magnitudes.

ii) Maximum current or kVA limits on network components such as transformers, overhead and underground lines, line recloser/regulators, and switches.

b) Var Control Active: If power factors are not an objective function variable, minimum power factor limits at each power delivery and supply point of interest.

c) Volt Control Active: If MW load demands are not an objective function variable, maximum MW load demand for each substation and/or power system network of interest.

The Dispatcher shall be able to execute VVC on demand. It shall be capable, however, of executing automatically in real-time at regular intervals (typically every 15 minutes) definable by the Dispatcher. On each execution VVC shall assess the current power system condition and determine the control actions that should be taken. Normally, these control actions shall be presented to the Dispatcher as a recommendation. The Dispatcher shall be able to accept the recommended control actions and have them automatically issued by the SCADA subsystem. As a Dispatcher option, VVC shall be able to issue the recommended controls automatically without waiting for Dispatcher approval.

VVC shall use the appropriate HV and/or MV network model to automatically find, for example, the capacitors, transformers, and DERs to be considered for control.

The Dispatcher shall be able to suppress VVC analysis and control on a substation-by-substation basis as well as prevent VVC from considering control of individual capacitors, transformers, line recloser/regulator devices, DERs, or SVCs.

In the case of equally sized parallel capacitor banks in substations, VVC shall give preference to operating the bank with the lowest operation count to keep the number of operations of each bank reasonably balanced.

20.21 DERMS Functionality

As an ever-increasing penetration of distributed energy resources (such as Solar-PV) is anticipated, the Authority foresees the need for a future Distributed Energy Resource Management System (DERMS) that will allow such resources to be controlled in coordination with the TDMS. Some DER control capability is already incorporated into the VVC function (refer to Clause 20.20.3). This assumes, however, that individual DER units are equipped for TDMS monitoring and control and supported by the necessary communications infrastructure, which currently is not the case.

Consequently, based on Contractor capabilities and experience, the Authority requires the Contractor to have proposed and described in detail a more comprehensive DERMS functionality that may be available and, as an option, could be fully integrated with the TDMS at a future date when the penetration level of DERs and the rules governing their interconnection requirements are more clearly defined. This may include enhancements to appropriate TDMS functions, such as the VVC, or the provision of a separate DERMS that would interoperate with the TDMS via a standard or proprietary interface.

20.22 Microgrid Interface Control

The Authority is planning for a microgrid that is expected to be operational within the next year or two. In the future, additional microgrids can also be expected. The TDMS, therefore, shall include a Microgrid Interface Control (MIC) function, which may be an extended form of the Volt/VAR Control function.

The MIC function shall enable the Authority's distribution network to supply power to microgrids in grid-connected mode such that the losses in associated feeders are minimized and the voltages and power factors at microgrid points of connection are kept within limits consistent with microgrid operational requirements and the need to avoid voltages that would exceed equipment ratings. The desired power and voltage signals for each microgrid will be provided by the microgrid's local controller and sent to the MIC function via a Feeder Device Control Unit (FDCU) or Feeder Remote Terminal Unit (FRTU). Provided by others, the FDCU/FRTU will be located at the microgrid's point of connection.

Responsibility for connecting a microgrid to the distribution network, i.e., transitioning from island mode to grid-connected mode, shall be possible using the MIC function. This responsibility may also fall to the microgrid's local controller. In the event the MIC function is given the responsibility, it must check before sending a close command to the switch at the microgrid point of connection that the

voltages on each side of the switch are synchronized at acceptable levels and nominal frequency. It must also ensure that the increase in load will not cause any voltage and/or overload problems.

Furthermore, in a planned transition from grid-connected mode to island mode, the MIC function shall also be capable of sending a control command to open the switch at the microgrid point of connection. This shall be preceded, however, by an analysis that will be used to set the distribution network in a state to avoid any significant voltage problems once the microgrid load is dropped.

Under certain conditions, the MIC function shall also be capable of sending a control signal to the FDCU/FRTU that will result in the non-planned disconnection of a microgrid. The conditions that the MIC function shall use to trigger such disconnection shall include:

1) Voltage at microgrid point of connection falls outside user predefined limits.

2) A fault internal to the microgrid occurs that is not cleared within a user predefined time limit.

20.23 Operations Simulator

The Operations Simulator (OPS) function shall provide an environment within which Dispatchers (or other authorized personnel) working at remote client workstations can execute TDMS real-time and study functions in simulation mode. In this respect, OPS may be used for training, testing applications and database changes, developing operating procedures, and investigating power system behavior as observed and recorded during actual power system operations. Also, to this end, OPS shall provide convenient to use features that will help users to set up and manage simulation scenarios, provide simulation oversight and control, and replay simulations.

Thus, to support the Authority's functional requirements, OPS shall include as a minimum:

1) A power system simulator capable of replicating the behavior of the power system during execution of dynamic time-dependent scenarios.

2) A scenario builder that can be used to set up dynamic simulation scenarios based on power system conditions and events derived from real-time time operations as well as directly from manually entered information. Such scenarios may be pre-defined and/or adjusted manually during their execution.

3) Ability to execute TDMS real-time and study mode functions (or replicas of these functions) in such a way that they can be used to monitor and control the simulated power system (rather than the actual power system) under conditions dependent on whatever dynamic scenario is being applied.

4) User interfaces for simulation setup, management, and review as well as those that replicate the user interfaces of the on-line TDMS.

20.23.1 OPS Utilization Facilities

OPS shall be capable of being utilized to support two (2) different utilization facilities. One of these shall be in the form of a Distribution Training Simulator (DTS), in which Dispatchers work through training sessions, i.e., as Trainees, under full supervision of a Trainer. The other shall constitute a self-training/study facility in which authorized users can run the OPS without supervision. These two facilities are further described as follows:

1) **Supervised DTS Facility** – This facility shall include one (1) Trainer remote workstation and six (6) Trainee remote workstations allowing access to the OPS for formal training purposes. These remote workstations supplied by the Contractor shall be installed with all necessary software at the Authority's Training Center, which is in a building close to the ADDC in Area C3. The facility shall allow an Authority-designated Trainer to run training sessions for up to six (6) Trainees at a time, where each Trainee (as in normal control room operations) may be assigned one or more AORs and a specific TDMS user role.

2) **Non-Supervised Self-Training/Study Facility** – This facility shall allow the Dispatcher (or any other authorized user) at any of the remote workstations in any of the Authority control centers to set up, monitor, and control a simulation session as well as execute the TDMS functions in their simulation mode.

Within this context, it shall be possible to run as many separate OPS sessions in parallel as the TDMS allows. This shall be no less than the minimum number of control room and DTS users as defined in Exhibit 15-8.

20.23.2 Dynamic Power System Model

The power system simulator shall be supported by a Dynamic Operations Model (DOM) that shall be an extended form of the Network Operations Model (NOM). Also, refer to Clause 20.5.

The NOM component of DOM shall include the data used for the power system model supporting the TDMS functions as used in their operational (on-line) real-time and study modes. Otherwise, DOM shall include settings, parameters, and all other modelling details as required to simulate the power system's behavior under user-defined operating conditions.

As a minimum, OPS capabilities and features shall support:

1) Simulations consistent with modelling the behavior of the power system from a static and dynamic perspective.

2) Creation of scenarios from pre-stored load curves and event groups, where event groups consist of one or more events that occur at the same time, at different times, or in accordance with other events and power system conditions.

3) Definition of events such as changes to bus loads, changes to system load, loss of generation, circuit breaker trip/close operations (including, for example, those corresponding to sustained line faults that result in breaker lockout and those corresponding to momentary faults that are

cleared by breaker reclose action), fault indications at one or more remote controlled switches, loss of FDI data, equipment alarms, etc.

4) Initialization from on-line TDMS save cases and snapshots of the real-time state of the actual power system.

5) Initialization from save cases and snapshots of the current state of the simulated power system derived, for example, from the result of executing the TDMS State Estimation function in its simulation mode.

6) Simulation starts, pauses, restarts, and stops.

7) Creation, application, and omission of events during an on-going simulation.

8) Periodic and demand snapshot save cases. At user discretion, periodic snapshots shall be saved automatically at a specified time interval throughout the simulation, where a snapshot is all data required to initialize the simulation to the conditions prevailing at the time of the snapshot. Periodic and demand snapshots shall not cause the simulation to pause and, in this respect, shall not disrupt user monitoring and control of the simulated power system.

9) Recording of scenario events so that these events together with a corresponding snapshot may be used to replay and review the simulation session.

The power system simulator's modelling shall extend to all equipment and devices comprising the power system as modelled in the on-line TDMS. It shall also extend to equipment and devices that are not included in this model but, as part of the power system infrastructure, affect the dynamic behavior of the power system.

The power system model as used by OPS shall also be capable of being modified in any way to represent the addition and/or removal of equipment and devices, as for example to study the impact of new substation construction.

Within this context, as a minimum, the power system simulator shall include models that can represent:

1) Time-dependent changes in bus loads as derived, for example, from the profiles of conforming and non-conforming loads for each effective season and day type. Users shall be able to modify such profiles, e.g., by defining a new peak value that scales the entire load profile, or by changing one or more individual load values. This shall include the capability to define and save load profiles manually.

2) SPP and VSPP distributed generation such as Solar-PV and wind-turbine renewable energy plant.

3) Power system frequency and/or voltage dynamics such as those that control the behavior of:

    a) Loads defined as functions of frequency and/or voltage.

    b) Overvoltage and undervoltage relays.

c) Overfrequency and underfrequency relays.

d) LTC transformers and generator AVRs.

4) SCADA functionality as, for example, opening and closing circuit breakers and disconnecting switches, sending set points and tap positions to control the power system's LTC transformers, and sending commands to reset underfrequency and lockout relays.

5) Overcurrent and automatic recloser relays in addition to the above referenced voltage and frequency relays.

6) Load Shedding in response to underfrequency relay operations.

20.23.3 Scenario Builder

Scenario definition and building to prepare for a training session or any other OPS session shall be supported by comprehensive and convenient user interface facilities. In this respect, a Scenario Builder shall be used to define scenarios that are up to twenty-four (24) hours long. Provisions shall be made to define multiple training scenarios. Scenario executions shall be recorded. This shall include a record of all Dispatcher and/or Trainer actions.

Each scenario shall be described by defining loads and events. This shall include the capability to define conditional and probabilistic events. Within this context, as a minimum, it shall be possible to create scenarios based on the following specifically defined events:

1) Circuit breaker/line recloser manual and automatic operation.
2) Trip or trip/close on circuit breakers/line reclosers.
3) Failure of circuit breakers/line reclosers to operate.
4) Relay malfunctions.
5) Local control malfunctions (such as applies to LTCs, load shedding, generation control).
6) Limit violations (all types).
7) Temporary and permanent loss of equipment (e.g., EGAT and SRTU data sources).
8) Loss of generation.
9) Changes in generator MW and Mvar outputs.
10) Single-bus load changes.
11) Area load changes.
12) Fault occurrence (e.g., a scenario defined event such as a feeder section fault resulting in a MV breaker trip).
13) Loss of lines or transformers.
14) Islanded operation.
15) Receipt of operational alarms.

16) Dispatching field crews.

17) Intermittent behavior of distributed energy resources such as Solar-PV and wind-turbine plant.

In addition to the above, the Scenario Builder shall support the merging of information available from the on-line TDMS to generate a scenario. For example, a scenario may be developed starting from an OPS scenario and subsequently merging IS&R data, including a power flow save case, from the on-line TDMS, i.e., OPS shall be able to be initialized by the IS&R. With each merge action, some data may be overwritten.

20.23.4 Simulation Management

The Contractor shall provide OPS user interfaces, including displays, control requests, and all other user interface activities, that are the same as those of the on-line TDMS. This shall include all associated user interface capabilities and features.

Also, as a minimum, the Contractor shall provide a user interface with all necessary functionality to support necessary simulation management capabilities. For example, these capabilities shall be designed to facilitate OPS training session setup and control. As such, the simulation management capabilities shall include:

1) Session start, stop, pause, and resume at any time within a scenario.

2) Session replay from an earlier state including all Dispatcher actions.

3) Variable real-time speed selection (fast, normal, slow).

4) Base case initialization from any of the following sources:

    a) Real-time snapshots from the on-line TDMS.

    b) Measurement data and save cases as existing on the on-line TDMS.

    c) Snapshots and save cases as created by OPS.

    d) Historic event data from the IS&R function.

5) Scaling of power system load for different operating conditions.

6) Saving multiple OPS save cases.

7) Scenario and associated initialization data storing in the OPS database. Scenario recall shall be preserved through power system model changes to the greatest possible extent.

All operations during an OPS session, including those of Dispatcher and/or Trainer, shall be logged automatically and shall be available for subsequent review.

In addition, the user shall be able to:

1) Create a library of training scenarios.

2) Initialize OPS with a snapshot saved during a training session.

3) After loading a snapshot, call up displays and examine any data normally available during a session as, for example, to review or discuss specific details with others.

4) Resume the simulation session from a snapshot in the same manner as resuming from a pause.

Reports for each session shall also be made available. As a minimum, these reports shall include the session log and any Trainer (or Trainer equivalent) comments that may have been incorporated during or after the session. Completed reports shall be capable of being saved, printed, and exported in a suitable format to other computer systems.

21. Documentation

Documentation shall be provided for all equipment and functions provided by the Contractor as part of DDIP. Unless otherwise specified in these Technical Specifications, all documentation shall be in English. The documentation shall describe the TDMS, including all of its hardware, software, and interfaces and shall cover functionality, testing, installation, cutover, system startup, operations, and maintenance.

21.1 Definitions

For the purposes of this project, the following definitions shall be used:

1) *Documents or Documentation* – Textural and graphical information describing the TDMS or equipment, systems, and other items peripheral to the TDMS, whether embodied in hardcopy or electronic form such as common word processor files. Documents may also be referred to as manuals, guides, books, drawings, transmittals, and specifications. Documents are further divided into standard, OEM, and custom documents.

2) *Standard documents* – Documents produced by the Contractor that are applicable to all users of the equipment and software, including the Authority. It is expected that the Contractor will use a formal revision control scheme to maintain its standard documents. Documents not maintained under such a scheme shall be considered custom documents.

3) *OEM documents* – OEM (original equipment manufacturer) documents are standard documents produced by subcontractors. Documents produced by subcontractors for customized elements of the TDMS shall be deemed custom documents.

4) *Custom documents* – All documents not categorized as standard or OEM documents including the Contractor's standard documents that are modified to meet the Authority's specific requirements.

5) *Project Documents* – Project documents are those documents produced for the conduct of the project, but which do not directly describe the TDMS. Examples of project documents include transmittal cover pages, correspondence between the Authority, the Contractor, and other

parties, electronic mail messages, records of telephone conversations, meeting minutes, action item lists, test plans and procedures, and transmittal and document lists.

The requirements for project documents are addressed in the following clauses:

1) Documentation plan – Clause 24.5.1
2) Project progress report – Clause 24.5.2
3) Project meeting, agenda, and minutes – Clause 24.5.3
4) Detailed implementation schedule – Clause 24.5.5
5) Project security documentation – Clause 24.6.1
6) Variance records – Clause 22.5.1
7) Factory test documents – Clause 22.4 and Clause 22.9
8) Site test documents – Clause 22.4 and Clause 22.10
9) Availability test documents – Clause 22.4 and Clause 22.11
10) Training documents – Clause 23.2.

The remainder of this clause addresses the requirements for documents other than project documents.

21.2 Document Format

Documents shall be delivered in two phases:

1) Approval documents submitted for Authority review and approval
2) Final documents.

In addition to accessing Contractor documents posted on the Project Tracking System (PTS) as described in Clause 24.4, the Authority prefers that documents be delivered as softcopy on magnetic media or by electronic transfer (electronic mail or ftp, for example). Final documents, as well as being posted on the PTS, shall be delivered as hardcopy and on CD-ROM.

System users with appropriate permissions shall be able to access system on-line documentation as well, i.e., documentation such as functional design documents, user guides, maintenance manuals, on-line help, and operating procedures, via a simple procedure involving a point and click operation.

Documents shall be supplied in a format that can be edited by the Authority. Handwritten texts are not acceptable. The Authority's standard word processing software is Microsoft Office. The Contractor is encouraged to use this software for documents. All documents should be searchable. If the Contractor uses other word processing or document production software, copies of the software suitable for installation on personal computers using a current Windows operating system shall be provided.

Drawings and diagrams may be embedded in the document files or may be supplied as separate files. The Authority's standard drawing software is AutoCAD. If the Contractor uses other drawing software, copies of the software suitable for installation on a personal computer using a current Windows operating system shall be provided.

Documents delivered as hardcopy shall be printed on both sides of A4 paper and bound in three-ring binders. Divider pages with appropriately labeled tabs shall separate chapters. The spine of each volume shall be labeled with the document title and volume number so it may be easily identified when shelved.

Documents delivered on softcopy media shall be formatted for printing on A4 paper.

Each document shall include a title or information page showing the document number, title, and revision record. The document number shall be a unique number assigned in accordance with the Contractor's standard practice. The title page shall include a space into which the Authority may enter a document number assigned from the Authority's document management system. The revision record shall describe each new version of the document since its original production. The revision record shall include:

1) The date of the change

2) A brief description of the change

3) An indication that the change has been reviewed and approved in accordance with the Contractor's quality assurance procedures

4) The version or release of the hardware or software to which the document applies.

Each document shall include a table of contents. If a document is divided into several physical volumes, each volume shall contain the complete table of contents of the whole document.

Documents that describe generic or typical TDMS elements will not be acceptable to the Authority unless the specific material applicable to this project is easily distinguishable from the material not applicable to this project. Custom documents shall not contain any material that is not pertinent to the project.

Where the phrase "on-line documentation" is used in these Technical Specifications, it shall be interpreted to mean the ability to view the document from any TDMS workstation. The Contractor shall provide all software necessary to provide this capability. For non-OEM documentation (documentation produced by the Contractor), the Contractor shall also provide the capability to edit and annotate the document.

21.3 Document Review and Approval

All standard and OEM documents provided pursuant to this contract shall be subject to review by the Authority. Custom documents pursuant to this contract shall be subject to approval by the Authority.

21.3.1 Document Review

The Authority's review of documents shall be limited to determining that:

1) The documents are legible and have been produced in accordance with the documentation standards of the Contractor or subcontractors.

2) All hardware and software is in full conformance with the contract.

3) All software has been produced in accordance with the coding and display standards of the Contractor or subcontractors.

4) The documents clearly and accurately describe the features and options of the hardware and software that pertain to the TDMS.

The Authority will review documents within ten (10) working days of their submittal. Unusual circumstances notwithstanding, if the Authority does not transmit comments on the documents within the review period, the Contractor may assume that the document is fully acceptable to the Authority.

If the Authority transmits comments on any documents, the Contractor shall respond to the comments within ten (10) working days of receipt of the comments. If the comments address OEM documents, the Contractor shall act as an advocate of the Authority to initiate and facilitate resolution of the comments with the subcontractor.

21.3.2 Document Approval

All custom and project documents shall be subject to a formal approval process. Factory and site test plans and procedures (Clauses 22.4.1 and 22.4.2) shall also be subject to approval. The review for approval performed by the Authority will be like the document review process, but will more closely examine the functionality and design aspects of the hardware or software. Clarity and completeness of the presentation of the material within the documents will be a key element of the review for approval.

The approval process shall proceed as follows:

1) The Contractor shall transmit documents subject to the approval process to the Authority. The transmittal cover shall identify the document as requiring approval and shall identify the date by which the Authority should respond. The Contractor shall allow at least ten (10) working days for the Authority's reading of the document. This time may be adjusted by mutual agreement to accommodate the other activities of the Authority and the Contractor. Requests by either party to change the time shall be made within two (2) working days of receipt of the documents by the Authority.

2) The Authority shall return comments to the Contractor within the agreed time. The transmittal cover for the comments shall clearly indicate that the document is either:

    a) *Approved* – If approved, the Contractor may proceed with the work covered by the document. No further approval action is required.

b) *Approved with Comments* – If approved with comments, the Contractor may proceed with the work covered by the document and the comments.

c) *Not Approved* – If not approved, the Contractor may proceed with the work covered by the document and the comments only at the Contractor's own risk. No schedule or cost relief will be granted for any work undertaken prior to approval of the appropriate documents.

3) If desired by any party, the comments may be discussed to clarify the Authority's intent.

4) The Contractor shall then revise and resubmit the documents within five (5) working days after receipt of the comments from the Authority. This time may be adjusted by mutual agreement to accommodate the other activities of the Authority and the Contractor. Requests by either party to change the time shall be made within two (2) working days of receipt of the comments by the Contractor.

5) All changes made to documents to reflect approval comments shall be clearly highlighted and the revision record shall be updated to reflect the changes. The Authority prefers the use of the change-tracking feature of the word processor used to produce the documents.

6) The review and comment process shall be repeated until the document is accepted. After the document is accepted, the Contractor shall deliver the required number of final copies free of highlighting due to the tracking of changes.

21.3.3 Scope of Reviews and Approvals

The acceptance or approval of any documents by the Authority shall not relieve the Contractor of the responsibility to meet all requirements of the contract including responsibility for correction of the documents. The Contractor shall have no claim for additional costs or extensions of time because of delays due to document revisions that may be necessary for ensuring compliance with the contract.

All deliverable documentation shall be revised by the Contractor to reflect the delivered TDMS. Any modifications to the TDMS resulting from the factory and site acceptance tests shall be incorporated in this documentation. 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.

Exhibit 21-1: Deliverable Documentation

Document	Quantity				Delivery Date
	Review and Approval		Final		
	Hard Copy	Soft Copy	Hard Copy	Soft Copy	
System Overview Document	3	1	2	2	One month after Award of Contract (AOC)
Documentation Standards	3	1	2	2	One month after AOC
Basic hardware documents • List of Deliverables,	3	1	2	2	• One month after AOC

Document	Quantity				Delivery Date
	Review and Approval		Final		
	Hard Copy	Soft Copy	Hard Copy	Soft Copy	
Configuration Diagrams • Network Configuration, Interconnection Lists • Site Installation Drawings and Procedures					• One month prior to delivery of the TDMS • Two months prior to delivery of TDMS
Equipment Manuals	3	1	2	2	With each hardware delivery
Hardware Maintenance Manuals	3	1	2	2	With each hardware delivery
Software list of deliverables	3	1	2	2	One month after AOC
Software Development Standards	3	1	2	2	One month after AOC
Database Definition • Standard Software • Other Software	3	1	2	2	• One month after AOC • Prior to FAT
Software Functional Description Documents	3	1	2	2	Prior to FAT
Installation Images and Source Code	3	1	2	2	With TDMS delivery
Software Requirements Matrix	3	1	2	2	Prior to FAT
Detailed Design Documents	3	1	2	2	Prior to FAT
Interface Requirements Document	3	1	2	2	Prior to FAT
System Maintenance Manual	3	1	2	2	With TDMS delivery
Cyber Security Document	3	1	2	2	Prior to FAT
Display Style Guide	3	1	2	2	Two months after AOC
Operating Manuals • Development System • DAC Simulator • TDMS Dispatcher's Manual • TDMS Database and Display Editor Manuals	3	1	2	2	• One month before delivery • One month before delivery • With TDMS delivery • Prior to FAT
As-Built Documents and Drawings	3	1	2	2	Per project schedule, but prior to TDMS acceptance

21.4 Deliverable Documentation

Exhibit 21-1 above lists the minimum documentation to be delivered, the quantities to be delivered, and the desirable delivery dates for first submission of the review and approval copies. The Authority will establish the distribution list for the copies after contract award.

The Authority recognizes that the documentation scheme used by the Contractor may not match the scheme described in this and other clauses. Therefore, the Contractor is not expected to supply the specific documents presented herein. The documentation supplied, however, shall provide all the information described in the following clauses.

21.5 System Overview Document

The Contractor shall provide a System Overview Document for each TDMS that introduces the reader to the purpose and function of the system. This document shall provide a basic description of the system and its functions, the relationship between the functions including the data flow between them, and the local and wide area communications networks used by the TDMS. Thus, as a minimum, the document shall include the following content:

1) Description of the system architecture.

2) Description of all functions with respect to

    a) User Interface.

    b) SCADA.

    c) Information Storage and Retrieval.

    d) Power System Applications.

    e) Database.

    f) Interfaces.

3) Description of associated local and wide area networks.

21.6 Documentation Standards

The Contractor shall provide a document defining the standards used to create and maintain all documentation supplied by the Contractor. The standards shall define:

1) The word processing or document production software used to create the documents

2) Templates for each document type

3) Definitions of the contents for each document type

4) Drawing standards to be followed

5) The approval process to be followed for document releases.

21.7 Hardware Documentation

The following documentation shall be provided for all hardware provided pursuant to this contract:

1) List of deliverable hardware

2) Equipment configuration diagram

3) Network configuration diagram

4) Interconnection list

5) Site installation drawings and procedures.

The other hardware documentation to be supplied shall be commensurate with the hardware maintenance philosophy to be employed by the Authority, which is to maintain all hardware after system acceptance using its own staff as much as possible (also refer to Clause 24.9 of these Technical Specifications).

Equipment manuals shall be provided for all hardware to be maintained by the Contractor or a third-party maintenance contractor. This documentation shall be that which is normally supplied by the OEM as long as it includes the information described in Clause 21.7.6.

Equipment manuals and hardware maintenance manuals shall be provided for all hardware to be maintained by the Authority.

21.7.1 List of Deliverable Hardware

The list shall itemize each hardware item and include equipment configuration information. The configuration information shall be sufficient so that the Authority can procure an identical item from the manufacturer. The list shall also include network names and addresses (or these shall be included in the network configuration diagram) and shall include a space for the Authority to enter equipment identification for their own purpose.

21.7.2 Equipment Configuration Diagram

The equipment configuration diagram shall depict the logical interconnection of all Contractor-supplied equipment and its connection to the Authority-supplied equipment. The configuration diagram shall use the same terminology as the list of deliverable hardware so that the correspondence between the two can be readily determined.

21.7.3 Network Configuration Diagram

This document shall show the design of the local area networks supplied by the Contractor as well as the associated local and wide area networks supplied by the Authority. Both logical and physical depictions shall be provided for the network supplied by the Contractor. Only a logical depiction is required for the network supplied by the Authority.

21.7.4 Interconnection List

The physical interconnections among the TDMS components, other than those shown on the network configuration diagram, shall be depicted. Each cable shall be identified, along with its terminations.

21.7.5 Site Installation Drawings and Procedures

The site drawings shall depict the physical arrangement of the TDMS components. References to the appropriate equipment manuals are acceptable. The drawings and procedures shall include:

1) Equipment physical drawings showing dimensions, cabinet internal arrangements, and the size and weight of each enclosure

2) Unpacking, moving, handling, and other installation details

3) The location of external connections including types and sizes of connectors

4) Input power and grounding requirements

5) Environmental requirements.

21.7.6 Equipment Manuals

Equipment manuals shall contain the following:

1) A description of the function of the equipment

2) Installation, setup, and operating instructions

3) A block diagram showing the logical and physical interconnections among the major components

4) Expansion and upgrade capabilities and instructions

5) Preventive maintenance instructions

6) Detailed functional, logical, electrical, and mechanical characteristics of all interfaces to the device, including protocol descriptions

7) Troubleshooting and repair guides including a description of and instructions for the diagnostics furnished.

21.7.7 Hardware Maintenance Manual

The hardware maintenance manual shall describe the preventive maintenance and restorative procedures required to maintain the equipment in good operating condition. The information in the manuals shall include:

1) *Operating details* – This information shall include a detailed description of how the equipment operates and a block diagram illustrating each major assembly in the equipment. Descriptions of external data transfers with other equipment, including data patterns, security check-codes, and transfer sequences shall be included. The operational sequence of major assemblies within the equipment shall be described and illustrated by functional block diagrams and timing

diagrams. Detailed logic diagrams shall also be provided as necessary for troubleshooting analysis and field repair actions.

2) *Preventive maintenance instructions* – These instructions shall include all applicable visual examinations, hardware testing and diagnostic routines, and the adjustments necessary for periodic preventive maintenance of the equipment. Instructions on how to load and use any test and diagnostic program and any special or standard test equipment shall be an integral part of these procedures.

3) *Corrective maintenance instructions* – These instructions shall include procedures for locating malfunctions down to the field-replaceable module level. These guides shall include adequate details for quickly and efficiently locating the source of an equipment malfunction. The instructions shall also include explanations for the adjustment or replacement of all items, including printed circuit cards. Schematic diagrams of electrical, mechanical, and electronic circuits, parts-location illustrations, photographs, cable routing diagrams, and sectional views giving details of mechanical assemblies shall be provided as necessary to replace faulty equipment. For mechanical items requiring field repair, information on tolerances, clearances, wear limits, and maximum bolt-down torque shall be supplied. Information on the loading and use of special off-line diagnostic programs, tools, and test equipment, as well as any cautions or warnings that must be observed to protect personnel and equipment shall be included.

4) *Parts information* – This information shall include the identification of each replaceable or field-repairable module. All other parts shall also be identified. The identification shall be at a level of detail sufficient for procuring any repairable or replaceable part. Cross-references between the Contractor's part numbers and the manufacturer's part numbers shall be provided.

21.8 Software Documentation

The following overarching documents shall be provided:

1) List of Deliverable Software.
2) Software Development Standards.

The Contractor or subcontractors shall also provide documents for all software that has been produced for the TDMS. This shall include:

1) Database definition documents.
2) Interface requirements documents.
3) Software functional description documents.
4) Installation images and source code.
5) Source code version control and revision control documentation.

In addition, the following documents shall be provided for all software produced specifically for this contract:

1) Software requirements matrix.

2) Detailed design documents.

21.8.1 List of Deliverable Software

The list shall itemize each software item and include version and license information. The distribution media for each software item shall be identified. The list shall also indicate for each item whether source code is supplied.

21.8.2 Software Development Standards

The Contractor shall document the development standards used to develop the TDMS software. The Authority reserves the right to reject software that does not conform to the development standards. The standards shall define:

1) Program design disciplines

2) Resources under which the program must operate

3) Basic services

4) Interface definitions

5) Linkage conventions

6) Input and output specifications

7) Database naming and access conventions

8) Storage rules

9) Quality assurance procedures

10) Configuration design review methods

11) Software configuration control schemes.

21.8.3 Database Definition

The database definition shall identify the characteristics of all TDMS databases. It shall include, but shall not be limited, to the following:

1) The name or identification of the database

2) A description of the intended use of the database. If the database is specific to a single application, the application shall be identified.

3) A description of the organization of the database (the database schema or model)

4) A description of each field of each data item

5) Instructions for generating and populating the database

6) Details of programming interfaces. This shall encompass access methods, address schemes, and read, write, and modify actions.

7) Initialization description (how, or by what software, data is initialized and to what values)

8) Details of maintenance actions.

The Authority encourages the use of "self-documenting" database technology, where the database definition is developed and stored with the data. The resulting documentation should be printable.

21.8.4 Software Functional Description

The intent of the software functional descriptions shall be to describe the functions to be performed by each software module from the standpoint of a user. Software functional descriptions are also referred to as user guides. The functional operation of the TDMS shall be clearly described so that it can be understood without understanding the detailed operation of each software module.

Software functional descriptions shall also be used as the first step in the design of custom applications or features (for example, new functionality). They shall have sufficient information for the Authority to determine that the new functionality will meet the requirements of the contract.

The software functional descriptions shall include the following minimum content:

1) *Functional description* – A narrative description of each program. Where appropriate, solution algorithms shall be described.

2) *Performance requirements* – The execution periodicity, processing capacity, and tuning and execution parameters that control or limit the capabilities of the software.

3) *Resource requirement* – The expected minimum requirements for main memory, auxiliary memory, processor capacity, and other resources required by the software.

4) *User interface* – A description of the interface used to control the software, including all user inputs and program responses.

5) *Software interface requirements* – A description of the logic interfaces with other programs.

6) *Data requirements* – A description of all data and databases accessed by the software, including execution parameters.

7) *Error messages* – A concise description of all error messages and possible corrective actions.

8) *Diagnostic messages* – Where the software generates a record of its internal operations, the messages shall be described.

9) *Maintenance and expansion procedures* – A description of either maintenance procedures or expansion procedures that is relevant to maintenance of the program or expansion of the program.

It is the Authority's strong preference that software functional descriptions are provided as on-line documentation.

21.8.5 Installation Images and Source Code

All software shall be delivered in three forms:

1) As a fully operational system installed on auxiliary memory

2) As distribution images that are suitable for installation on the system

3) Buildable source code including libraries, compilers, and linkers for building software.

The distribution images shall include all operating system, platform software, application software, and the code management library of modifications incorporated into the delivered software. All standard software shall be supplied on the original installation media used by the Contractor to build the system. The Authority prefers CD-ROM as this media. All customized software shall be supplied as part of the code management library along with the source code or other distribution image against which the code changes are to be applied.

It shall be possible for the Authority to completely generate, build, install, and configure the entire TDMS from the distribution images, source code, and software utilities provided with the TDMS. To this end, "make files" or other compilation, generation, and installation tools, scripts, and directives shall be delivered.

For the purposes of this requirement, "software" shall specifically include the databases supplied with the TDMS, i.e., sufficient definition and content images shall be supplied such that the databases can be created and installed on the TDMS.

21.8.6 Software Requirements Matrix

The Contractor shall provide a list of all software requirements, cross-referenced to show where each requirement is discussed in the relevant software document.

The Software Requirements Matrix shall list each of the requirements for the TDMS stated in this specification, in numerical order, referenced by chapter, clause, and paragraph number. This list of specified requirements shall be supplemented by a list of all functions provided by the Contractor’s software system that go beyond the specified requirements.

For each requirement on the list, a reference shall be given to the chapter and clause where the requirement is described or covered in each of the following Contractor documents:

1) List of Software Deliverables

2) Software Functional Description

3) Operations Manual

4) Factory Acceptance Test

5) Site Acceptance Test.

21.8.7 Detailed Design Document

The detailed design documents are intended as a second level of detail to the software functional descriptions. In general, a detailed design document shall relate to a single software functional description. It is expected that, for customized software, the Contractor will first deliver a software functional description for approval by the Authority. After approval, the Contractor will produce a detailed design document for approval. Production of the software will then proceed after approval of the detailed design document.

The detailed software design documentation shall include, but shall not be limited to, the precise design information needed for planning, analysis, and implementation of the software. 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, and a detailed design description containing the internal details of each design entity.

The detailed software design documentation shall provide a detailed description of how the software will support the functions described in the software functional description. Detailed software design documentation shall include a diagram of the software indicating major modules and an overview of the operation of each module. It shall describe data structures and flow and a diagram or description of the way in which the modules interface with other modules.

For each software module, the detailed software design documentation shall include, but shall not be limited, to the following items:

1) Program abstract

2) General technical description of the module

3) The module logic (the use of pseudo code or structured English is preferred)

4) External interfaces to the program including applicable calling sequences

5) Initialization considerations

6) Identification of any databases referenced or modified

7) A high-level flowchart or program design language to enhance the technical description of the module

8) Error codes and error handling processes.

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

Authority personnel to maintain such software in the future. 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 detailed software design documentation.

21.9 Interface Requirements Document

The Interface Requirements Document shall describe in detail the interfaces between the TDMS and Authority-provided systems and networks. Both the Contractor and Authority will use the Interface Requirements Document as the definition of the interface between the TDMS and all other systems, so that each system can be designed or modified to meet its requirements. The Authority will provide all required information to the Contractor so that it can prepare the document accordingly.

As a minimum, the Interface Requirements Document shall cover the following aspects:

1) Description of the hardware interface.

2) Description of the communication protocols, including the lower level network protocols, the upper level session, presentation, and application protocols, and the options and parameters selected.

3) Description of the database access methods and capabilities, including specific displays, commands, and access and authorization requirements.

4) Description of relevant database models, structures, and contents for these databases.

5) Data exchange requirements including timing, priority, volume, and security requirements. A specific list of data to be exchanged during factory and site testing shall also be included.

6) Description of the performance requirements.

7) Exception (for example, error) processing.

8) Failover/backup processing.

9) Alarm conditions.

10) Archiving requirements.

21.10 System Maintenance Manual

The System Maintenance Manual shall describe all user procedures necessary to build and maintain the software system of the TDMS. It shall include complete instructions on performing a system generation from sources for all processors. It shall provide information on optimizing system performance. It shall describe the hierarchy of disk directories used by the TDMS software system, and the location of all categories of files: including executable programs, displays, databases, sources, build files, etc. It shall also describe the procedures to configure the TDMS computer system.

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.

The manual shall provide a list of the Internet Protocol (IP) addresses of all devices in a manner compatible with the Authority's security standards and shall describe the procedures for upgrading or adding additional workstations, loggers, storage devices, and other peripheral devices.

The System Maintenance Manual shall provide detailed information on troubleshooting all processors of the TDMS. 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. 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. It shall include a description of the procedures to restore normal operation after a failure of the TDMS.

The maintenance manual shall detail the procedures to back up the TDMS software, configuration data, and operating data, and shall present a schedule for periodic backup. Directions to restore software, configuration data, and operating data for each server and workstation shall also be provided.

21.11 Cyber Security Documentation

The Contractor shall produce documentation of all network configurations, including network access control rules implemented in "firewalls" used to secure the electronic perimeter(s) surrounding the component systems of the TDMS. The documentation shall include a description of all systems that interact electronically with the TDMS and describe the purpose and justification for all interconnections, including whether they are required for core operations, business information needs, or maintenance. Additionally, this document shall include the network address, protocol service, and direction of initiation for each documented access.

21.12 Display Style Guide

The Contractor shall furnish a Display Style Guide that describes the discretionary aspects of display design and implementation. This guide shall take into consideration the Authority's existing EMS/DMS display conventions and standards. The resulting Display Style Guide shall be used by the Contractor to develop all displays supplied with the TDMS. The display conventions and standards shall promote a consistent look and feel across all TDMS displays.

21.13 Operating Manuals

The Contractor shall submit, for review and approval, operating manuals for all TDMS functions. The operating instructions associated with all features shall be incorporated into these manuals. Context sensitivity shall be used to go directly to the appropriate place in the manual.

The manuals shall be organized for quick access to each detailed description of the user procedures that are used to interact with the TDMS functions. The manuals shall present in a clear and concise manner all information that a user needs to know to understand and operate the TDMS satisfactorily. The manuals shall make abundant use of monitor snapshots to illustrate the various procedures.

21.13.1 Dispatcher's Manual

The Dispatcher's Manual shall be custom documentation written specifically for the TDMS as finally delivered and accepted by the Authority. All snapshots used as illustrations shall be of genuine displays on the actual TDMS.

The Dispatcher's Manual shall be written for use by the Authority's Dispatchers. It shall be organized in a logical sequence and shall fully describe the user interface relevant to all operational functions of the TDMS. 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.

The manual shall describe the TDMS in a manner and at a level of detail that allows the user to detect and isolate problems in the TDMS. 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.

The Dispatcher's Manual shall be provided on-line. The Dispatcher shall be able to access the manual from a workstation using a simple one-click approach.

21.13.2 Database Editor's Manual

The Database Editor's Manual shall describe the procedures to define, build, edit, archive, and expand all the databases of the TDMS. It shall contain information describing how a user may define and add new attributes to an existing database entity. It shall also describe how to restore any database to a previously saved version if the database becomes corrupted.

The Database Editor's Manual shall describe the procedures used to import data from the Authority's GIS, validate this data, and then use it to populate the TDMS database.

The Database Editor's Manual shall document development of models such as those used by the power system applications described in Clause 20 of these Technical Specifications. This shall include the building of scenarios for use by TDMS functions when running in simulation mode.

The Contractor shall provide documentation that describes the Contractor's implementation of CIM. This documentation shall include the following:

1) The detailed model definitions and objects

2) Maintenance manual

3) User's toolkit guide.

21.13.3 Display Editor's Manual

The Display Editor's Manual shall describe and fully illustrate the capabilities of the Display Editor, including procedures to auto-generate and edit single-line displays for the TDMS and to link display fields with entities in the database of the TDMS. It shall describe how to generate new device symbols. 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 to achieve a satisfactory decluttering upon zooming.

The Display Editor's Manual shall describe the procedures used to create schematic one-line overview displays from Authority AutoCAD drawings and geographical one-line overview displays from GIS data. The procedures used to link these schematic and geographical displays shall also be described. Where applicable, the capability to generate schematic displays from geographical displays automatically shall be described. The Contractor's proposal shall have identified if this capability is available as part of the Contractor's standard offering.

21.14 As-Built Documents and Drawings

The Contractor shall submit as-built documents including applicable drawings for review and approval. All deliverable documents and drawings shall be revised by the Contractor to reflect the as-built TDMS. Any errors in or modifications to the system resulting from the factory and site acceptance tests shall be incorporated in this documentation. Within this same context, all previously submitted documents that are changed because of engineering changes, contract changes, or errors or omissions shall be resubmitted for review and approval.

22. Quality Assurance and Testing

To ensure that the Contractor produces a well-engineered and contractually compliant TDMS, a quality assurance program shall be followed and both structured and unstructured tests shall be performed. This program shall include the early integration tests in cooperation with the suppliers of the FDCU and radio equipment, i.e., as part of the required Joint Development program (refer to Part A of these Technical Specifications), the ability of the TDMS to interoperate successfully with the FDCU and radio equipment shall be demonstrated. This is to minimize potential problems during on-site point-to-point testing, problems such as those associated with communications, point mapping, and the protocol profiles implemented by the project's different FDCU suppliers.

22.1 Quality Assurance Program

The Contractor shall employ documented Quality Assurance (QA) techniques and practices throughout this project. This QA program shall cover the preparation of all contract deliverables, including documentation, hardware, and software. The program shall provide for the minimization of defects, the early detection of actual or potential deficiencies, timely and effective corrective action, and a method to track all such deficiencies.

22.2 Inspection

The Authority shall be allowed access to the Contractor's facilities during system design, manufacturing, and testing and to any facility where hardware or software is being produced. The Contractor shall provide office facilities, equipment, and documentation necessary to complete all inspections and to verify that the TDMS is being fabricated and maintained in accordance with the Technical Specifications.

The Authority shall be allowed to review and verify the functional implementation of TDMS software informally in conjunction with scheduled project meetings at the Contractor's facilities. No test plans, procedures, or reports are required to support these informal software demonstrations.

The Authority shall be allowed to inspect the Contractor's hardware and software quality assurance standards, procedures, and records. Documents that are identified in the approved software quality assurance plan will be inspected to verify the Contractor has performed the required quality assurance activities.

The inspection rights described above shall not apply to subcontractors supplying standard computer or peripheral equipment and third-party software products. Inspection rights, however, shall apply to subcontractors that are developing new software for inclusion in the TDMS.

22.3 Test Responsibilities

In writing and prior to the start of factory testing, the Authority and Contractor shall each designate a test coordinator. To ensure tests are conducted expeditiously, in accordance with Authority requirements, the coordinators shall have the authority to make binding commitments. This shall include, for example, the approval of test results and the scheduling of variance corrections.

The Contractor shall be responsible for all factory tests. This responsibility shall include the conduct of the tests and all record keeping and document production. The Authority will support the factory testing by supplying staff to witness and help execute the test procedures under the Contractor's supervision.

The Contractor shall also be responsible for all site tests prior to the Guarantee Test that will be conducted by the Authority under typical system operating conditions. During the Guarantee Test (refer to Clause 24.8), the Contractor shall provide support by supplying at least one suitably experienced staff member to assist the Authority as well as monitor the test.

The TDMS will be maintained throughout testing commensurate with the requirements of Clause 24.9 of these Technical Specifications.

22.4 Test Documents

Test plans, procedures, and records shall be provided by the Contractor for all tests (excluding inspections and software demonstrations pursuant to Clause 22.2) to ensure that each test is comprehensive and verifies the proper performance of the TDMS elements under test. During the development of test plans and test procedures, emphasis shall be placed on testing each functional requirement, checking error conditions, and documenting the simulation techniques that may be used. The test plans and test procedures shall be modular to allow individual test segments to be repeated as necessary.

All test plans and test procedures (standard, modified standard, and custom functions) shall be submitted to the Authority for approval and shall be subject to the approval process as defined in Clause 21.3.

22.4.1 Test Plans

The test plans shall describe the overall test process, including the responsibilities of individuals and the documentation of the test results. The following shall be included in the test plans:

1) The schedule for the test.

2) The responsibilities of Contractor and Authority personnel, including record-keeping assignments.

3) Any forms to be completed as part of the tests and the instructions for completing the forms.

4) Procedures for monitoring, correcting, and testing variances.

5) Procedures for controlling and documenting all changes made to the hardware and software after the start of testing.

6) Block diagrams of the hardware test configuration, including the field device interfaces provided by others, external communication channels, and any test or simulation hardware.

Test plans shall be provided for the Factory Acceptance Test, Site Acceptance Test, and System Availability Test.

22.4.2 Test Procedures

The test procedures shall describe the methods and processes to be followed in testing the TDMS. The test procedures shall be modularized, such that individual functions of the TDMS can be independently tested and so that the testing proceeds in a logical manner. This clause 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.

The test procedures shall include the following items:

1) The name of the function to be tested.

2) References to the functional, design, user, and any other documents describing the function.

3) A list of test segments to be performed and a description of the purpose of each test segment.

4) The setup and conditions for each segment, including descriptions of the test equipment and data to be supplied by the Contractor and by the Authority.

5) Descriptions of the techniques and scenarios to be used to incorporate as well as simulate field device interfaces and connections to external networks and systems.

6) Descriptions, listings, and instructions for all test software tools and displays.

7) Step-by-step descriptions of each test segment, including the inputs and user actions for each test step.

8) Forms for the recording of test results.

9) The expected results for each segment, including pass/fail criteria.

10) Copies of any certified test data to be used in lieu of testing.

The Contractor shall note that the Authority will not accept any certified test data in lieu of testing except where specifically stated in the contract.

22.4.3 Test Records

Complete records of all tests result shall be maintained. The records shall be keyed to the test procedures. The following items shall be included in the test records:

1) Reference to the appropriate test procedure.

2) Date of the test.

3) Description of any test conditions, input data, or user actions differing from those described in the test procedure.

4) Test results for each test segment including a passed/failed indication and a record that each step was performed. All information recorded during the test such as measurements, calculations, or times shall be included in the results.

5) Identification of the Contractor and Authority representatives performing and witnessing the test.

6) Provision for comments by the Authority representatives.

7) References to all variance reports generated.

8) Copies of reports, display copies, and any other hardcopy generated as part of the test.

22.5 Variance Recording and Resolution

The Contractor shall establish a process to record and track variances. This process shall be initiated at a time to be determined by the Contractor, but no later than the start of pre-FAT, and shall continue through the completion of the warranty. Both the Contractor and the Authority may initiate variances at any time. Variances may be used to record system deficiencies, including:

1) Documentation deficiencies.

2) Functional deficiencies.

3) Performance deficiencies.

4) Procedural deficiencies (as when deviations from contractually required QA procedures are observed).

5) Test deficiencies (as when the system cannot satisfactorily complete a test procedure due to a problem with the test).

The variance process 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. Variance reports shall be available to the Authority always. The Contractor shall periodically distribute a variance summary that lists for each variance the report number, a brief overview of the variance, its category, and its priority.

22.5.1 Variance Records

The record of each variance shall include the following information:

1) The time and date of the initial discovery of the variance.

2) A variance number – a unique, sequential number assigned when the variance is entered into the tracking system.

3) An identification of the person submitting the variance and the names of any other witnesses or knowledgeable Authority or Contractor staff.

4) An identification of the TDMS component, such as a hardware item or software function, against which the variance is being written.

5) An identification of the test plan or procedure, if applicable. The stage or step of the plan or procedure shall be identified.

6) An overview of the variance suitable for use in keyword searches.

7) A detailed description of the variance.

8) A variance category:

    a) Open (recorded but not scheduled for further action)

    b) Assigned (scheduled for further action)

    c) Pending (the variance has been resolved but not tested)

    d) Closed (the Authority has accepted the resolution)

    e) Disputed (Contractor believes the reported problem is acceptable)

    f) Deferred (the variance will be corrected at a later project phase)

9) The date of assignment into each category.

10) A variance priority:

a) ***Critical*** – To be used only if the TDMS is in commercial use, this priority identifies a problem that prevents the use of a TDMS feature that is essential to the Authority's operation of the power system.

b) ***High*** – Denotes the failure of the TDMS to perform a required feature in a manner that significantly reduces the utility of the TDMS or feature or which delays further testing of the TDMS or feature.

c) ***Normal*** – Denotes the failure of the TDMS to perform a required feature in a manner that reduces the utility of the TDMS or feature. Normal priority variances shall not delay any testing.

d) ***Low*** – Denotes the failure of the TDMS to perform a required feature in a manner that reduces the utility of the TDMS only slightly. Low priority variances shall not delay any testing. Variances that record transient failures, that is failures that cannot be readily reproduced, shall be initially assigned to this priority. Subsequent occurrences of the transient failure shall result in raising the priority of the variance.

11) A description of the resolution, including identification of all hardware, software, and documents modified or otherwise changed and the names of the Contractor or Authority staff involved with the resolution.

12) A record of all testing performed.

13) Identification of the Authority staff accepting the resolution and the date of acceptance.

22.5.2 Schedule for Variance Correction

The Contractor and the Authority shall meet as necessary to review the variance list. Each new variance opened since the previous meeting shall be scheduled for correction at the meeting. The Authority and Contractor shall follow these guidelines for scheduling corrections:

1) A schedule for the correction of critical and high priority variances shall be set within one working day of their discovery. The schedule for correction of all other variances shall be set within three working days of their addition.

2) The Authority and the Contractor shall assign resources for the correction of critical variances with the intent of correcting the variance within two working days of their opening.

3) The Authority and the Contractor shall establish a mutually agreeable date for the correction of high priority variances, with the overall objective of:

a) If the TDMS is in productive use, correcting the variances within one calendar week of their discovery.

b) Prior to the commencement of productive use, maintaining the overall project schedule.

4) The Authority and the Contractor shall establish a mutually agreeable date for the correction of normal priority variances, with the overall objective of:

   a) If the TDMS is in productive use, correcting the variances within one calendar month of their discovery.

   b) Prior to the commencement of productive use, maintaining the overall project schedule.

5) Low priority variances may be scheduled for correction at any time, but shall not exceed one calendar month as of their discovery.

22.5.3 Variance Resolution

A variance shall be deemed resolved only upon written acceptance of the correction by the Authority. Prior to submitting the corrected variance for acceptance by the Authority, the Contractor shall take all reasonable steps to verify that the correction has resolved the variance, and the Contractor shall update the variance record to reflect the corrective action taken. The Contractor shall then schedule any testing to be performed in conjunction with the Authority.

A variance shall be deemed accepted only after the Authority has tested the corrected variance to its satisfaction. The Contractor shall support all testing deemed necessary by the Authority to verify the corrections.

22.6 Test Schedule

The sequence of tests to be performed and their scheduling with respect to other activities are presented in Clause 24.7, Testing, Shipment, and Commissioning.

22.6.1 Test Initiation

The following conditions must be satisfied before starting any test (exclusive of inspections or demonstrations pursuant to Clause 22.2):

1) The Authority has approved all plans and procedures for the test.

2) The Authority has reviewed or approved all relevant documentation, including project documents.

3) A copy of all relevant documentation including design and maintenance documents, user manuals, test plans, and test procedures has been placed on the test floor.

4) A complete regeneration of the software under test, including databases and starting from source code, has been performed immediately prior to the start of testing.

5) All operating system parameters, files, and configuration information has been saved to archive media so that the TDMS operating environment can be recreated.

6) All database, display, and report definitions have been saved to archive media so that the databases, displays, and reports can be recreated if necessary.

7) All source code libraries have been saved to archive media so that TDMS software can be regenerated if necessary.

8) For the factory test, preliminary testing, as described in Clause 22.8, has been completed and the Contractor has submitted written certification accordingly.

9) For the system availability test, all critical, high, and normal variances have been corrected and verified to the satisfaction of the Authority.

22.6.2 Test Completion

A test shall be deemed to be successfully completed only when:

1) All variances have been resolved to the satisfaction of the Authority.

2) All test records have been transmitted to the Authority.

3) The Authority acknowledges, in writing, successful completion of the test.

22.6.3 Test Suspension

If the Authority 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. Repeating the test shall be scheduled for a date and time agreed upon by both the Contractor and the Authority.

22.7 Modifications to the TDMS during Testing

No changes shall be made to the TDMS after factory testing has started without the express authorization of the Authority. This requirement does not apply to pre-FAT. It is the Authority's intent to carefully control the test environment so that all changes can be readily identified and so that any changes installed for any purpose can be removed and the previous test environment restored. The Authority shall have the right to suspend testing, to revert to a previous version of any software or hardware, and to restart any testing previously performed if, in its opinion, changes have been made to the system under test without authorization.

22.8 Preliminary Factory Testing

Pre-FAT shall be a complete dry run of FAT, following the test plans and procedures. The intent is for the Contractor to detect and correct most design, integration, database, display, and performance problems prior to FAT. The Contractor's project manager shall sign off on each test. The completed test results shall be sent to the Authority for inspection before Authority personnel travel to participate in FAT at the Contractor's facilities. All tests shall be conducted using Authority-specific databases unless the Authority authorizes the Contractor to use a test database.

The Contractor shall notify the Authority at least thirty days prior to the start of the TDMS pre-FAT, and the Authority shall have the option to witness all or parts of it. The Contractor shall notify the Authority when the pre-FAT has been successfully completed and the TDMS is ready for FAT.

22.9 Factory Test

Factory tests shall include:

1) Equipment test

2) Functional test

3) Performance test

4) Stability test

5) Unstructured test.

22.9.1 Equipment Test

The equipment test shall verify that the TDMS includes all required equipment, that the equipment is properly configured, and that the equipment can successfully execute the diagnostic programs provided.

The equipment tests shall include a visual inspection for proper workmanship, including cables, connectors, and labeling. The assembly drawings and configuration drawings shall also be verified at that time. These tests shall also verify that the required TDMS capacity and expansion requirements of Clause 15 (Capacity and Performance) have been satisfied.

22.9.2 Functional Test

The functional test shall use an equipment configuration that may include an extension of the Contractor's deliverables as required to prove the correct functionality of the TDMS. The test procedures shall consider all additional test equipment and shall ensure that the additional equipment does not create false test results. 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 using the test data provided by the Authority, i.e., the specific data that represents the Authority's actual power system network. The use of substitute data representing a standard power system network, for example, is not acceptable.

All functional tests shall include the following:

1) Verification of all required functionality of the TDMS, such as SCADA, power system applications, data exchange, and information storage and retrieval. Verification shall include all standard and custom functions.

2) Verification that all software has been correctly sized and meets the Authority's capacity requirements.

3) 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 system.

4) Sample field device interfaces supplied by others shall be included in the testing. Where necessary, the Contractor shall provide appropriate simulations of external systems; such simulations must themselves be verified before being used.

5) Verification of all user interface functions.

6) Verification of the proper operation of local and wide area network devices, including bridges, routers, and gateways, and the entire network by monitoring network traffic using diagnostic procedures and reconfiguration tests.

7) Verification of the application program and system development capabilities including, software configuration management, source code development, documentation management, user interface development, real-time data set development, RDBMS development, database generation and maintenance, report generation and modification, alarm and event message definition, test environments, and other utility functions.

8) Verification of communications maintenance capabilities including diagnostics, field device interface data link maintenance, and local input/output maintenance.

9) Verification of all hardware maintenance capabilities.

10) Verification of the redundancy and failure recovery schemes of the system.

11) Verification of the proper response of the system to at least the following abnormal situations:

    a) Loss and restoration of processors and servers, including auxiliary memory

    b) Loss and restoration of user interface equipment

    c) Loss and restoration of archive storage devices

    d) Loss and restoration of external subsystems

    e) Loss and restoration of input power (UPS failure)

    f) Loss and restoration of communication network processors

    g) Loss and restoration of any other peripheral devices

    h) Loss and restoration of local and wide-area network elements

    i) Detection of and recovery from communication errors as simulated or otherwise demonstrated

12) Verification that changes of system time will not prevent the system from operating properly and that the system can correctly handle the beginning of a new day, month, and year, leap years, and changes in century and decade, etc.

13) Verification that all documentation to be delivered with the system is present and meets all applicable requirements.

14) Review and explanation of system error logs and unexpected alarms generated during the test.

22.9.3 Performance Test

The performance test shall verify that the specified performance requirements are met. Simulation shall be provided by the Contractor, where necessary, to create the conditions for the specified performance scenarios (refer to Clause15). The simulations shall be tested first to verify that the desired activity is being simulated. Execution of the performance tests shall be automated as much as possible so that test runs can be reproduced.

22.9.4 Stability Test

A 100-hour continuous run of the system shall be performed after successful completion of the functional and performance tests. The stability test will be considered successful if no critical function is lost, no major hardware failure occurs, no failover occurs, and no restarts occur within the test period.

Major hardware failure is defined for this test as the loss of hardware such as a processor, disk, user workstation, etc. Non-repetitive mechanical failures of printers, loggers, pushbuttons, etc., are not considered major failures. The test shall not purposely cause any hardware or software failure, i.e., failover and restart testing is not a goal of this test.

During this test, the system shall be exercised (with simulated inputs, events, and conditions) in a manner that approximates an operational environment. The Authority will help simulate unstructured user activity during this test. Otherwise, the Contractor shall take full responsibility for setting up and conducting the test.

22.9.5 Unstructured Test

The test schedule shall allow time throughout the functional testing for unstructured testing by the Authority. 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, but no less than four days total. This time will be used by the Authority to perform additional tests, the need for which may be recovered during the formal testing, and to investigate any potential problems detected. The unstructured tests will be performed during the functional and performance test period and during the stability test at the discretion of the Authority.

The Contractor shall assist the Authority in this test as required by the Authority; this assistance will be primarily in the form of helping to set up the test, explaining the best procedures to run the test, and explaining all unexpected results.

22.9.6 Cyber Security Audit

The cyber security audit shall verify that the requirements of Clauses 7, 11, and 24.6 and others have been satisfied. Within this context, as a minimum, the following cyber security test, verification, and review activities shall be conducted:

1) Review permissions and configurations to ensure that the deliverable configuration is accurately documented.

2) Verify that network traffic recoding and access recording have been enabled and are functioning.

3) Verify that unused services have been removed.

4) Verify that all software has been updated with the latest security patches.

5) Perform a virus and malware scan of the system and verify that all virus and malware scanning tools are enabled.

6) Verify that all "electronic self-help" software has been removed.

7) Regenerate all signature files and others used by the software integrity scheme.

8) Remove all generic and default accounts.

9) Verify that all access authorization methods are properly configured.

10) Review the currency of cyber security training and background checks for all Contractor staff to be sent to the field and all staff remaining at the Contractor's facility who will access or work on the TDMS.

11) Generate a full backup of software and databases.

22.10 Site Acceptance Test

The Site Acceptance Test (SAT) includes the installation test, the functional and performance test, and the cyber security audit that will be conducted at the Authority's site after Contractor shipment, installation, and pre-commissioning of the TDMS. In this respect, SAT shall constitute formal TDMS commissioning by the Contractor in the presence of Authority personnel as witnesses.

22.10.1 Installation Test

The installation tests shall be conducted by the Contractor and shall include:

1) A repetition of the equipment test of Clause 22.9.1.

2) Loading of the TDMS software and starting the system. At the option of the Authority, all software shall be recompiled from the source or distribution media.

3) In cooperation with the Authority, ensuring attachment of the TDMS to communications facilities for all data sources and other systems that interface with the TDMS.

4) Initialization and preliminary tuning of application software as needed.

22.10.2 Site Functional and Performance Test

The site functional and performance test ("site test") shall consist of a subset of the functional and performance tests of Clause 22.9.1, Equipment Test, Clause 22.9.2, Functional Test, and Clause 22.9.3, Performance Test.

The tests to be performed shall be proposed by the Contractor and approved by the Authority. These tests shall be extended as necessary to test functions simulated during FAT, such as communications with all field device interfaces and all other systems that interface with the TDMS. The extended tests shall be performed in accordance with a test procedure prepared by the Contractor and approved by the Authority. Unstructured tests shall also be employed, as necessary, to verify overall operation and responsiveness of the TDMS. In effect, the Contractor shall be responsible for demonstrating that the system can meet the Authority's specified capacity and performance requirements under actual field conditions.

Within this context, the site test shall include:

1) Verification of all TDMS interfaces with Authority-provided data sources and systems.

2) Verification of all TDMS interfaces with Contractor-provided data sources and systems.

3) Validation of TDMS databases, displays, and reports using field data.

4) Validation of the output of the TDMS functions (e.g., the SCADA and power system application functions) using field data.

22.10.3 Site Cyber Security Audit

The cyber security audit at site shall repeat the audit performed during factory testing (refer to Clause 22.9.6).

22.11 Availability Test

This test shall demonstrate TDMS and device availability in accordance with the criteria specified in Clause 14.8, System Availability.

22.11.1 Test Activity

The test activity shall consist of normal TDMS operations with the system in commercial use. The Authority may modify the TDMS databases, displays, reports, and application software during the availability test. Such modifications will be described to the Contractor at least 48 hours in advance of implementation to allow assessment of impact on the availability test, except where such changes are necessary to maintain control of the power system.

22.11.2 Test Definitions

The definitions of the time periods used in determining the duration of the test and the success of the test shall be as follows:

1) ***Downtime*** – Downtime occurs whenever the criteria for successful operation defined in Clause 14.8.2, Availability Requirements, are not satisfied. Downtime shall be measured from the start of diagnostic procedures until full service is restored. In the event of multiple failures, the total elapsed time for repair of all problems (regardless of the number of maintenance personnel available) shall be counted as downtime.

2) ***Hold time*** – Certain periods of time during which the TDMS is down may be due to circumstances that are beyond the control of either party. These contingencies may prevent successful operation of the TDMS, but are not valid for measuring availability. Such periods of unsuccessful operation may be declared hold time by mutual agreement of the Authority and the Contractor. Specific instances of hold time are:

    a) ***Scheduled shutdown*** – During scheduled shutdowns or times when equipment failure occurs while its backup device is scheduled out-of-service, the resulting system outage shall be hold time, if service can be restored per Contractor-specified procedures within 30 minutes.

    b) ***Power interruption and environmental excursion*** – Loss of power or manual shutdown of the TDMS in the event of power excursion or the loss of environmental control shall be considered hold time. If the TDMS is operated during periods of power or environmental conditions beyond those specified, any resultant downtime shall be considered hold time.

    c) ***Intermittent failure*** – Periods during which an intermittent, recurring failure is experienced will be considered hold time, if the Contractor is engaged in remedial action and normal operation of the TDMS can be restored within 30 minutes by Contractor-defined procedures whenever the failure occurs. Instead of accounting for the actual intermittent downtime, one hour of downtime shall be counted for each 120 hours of otherwise successful operation while the problem persists.

    d) ***Failure of Authority software*** – Time during which the TDMS is down due to failure of software written or provided by the Authority shall be considered hold time. (Programs developed by the Authority under Contractor supervision are specifically excluded from this provision.) If a failure in such software cannot be overcome by Contractor-defined procedures, execution of the failed program shall be suspended.

    e) ***Corrected design defect*** – Hold time may be declared by mutual agreement to ensure against similar future occurrences if a failure occurs due to a defect in design for which the Contractor defines and implements corrective measures. In such a case, sufficient hold time shall be allocated to allow verification of the corrective action.

f) ***Logistics delays*** – If repairs are delayed due to previous use of spare parts or because of the Authority's failure to purchase recommended spare parts, hold time will be declared after diagnosis of the failure and while the Contractor is pursuing replacement parts in an expeditious fashion. A maximum of 48 hours of hold time will be allowed for each occurrence of a logistics delay.

g) ***Service response time*** – Hold time shall be declared from the time that a failure is detected until diagnostic procedures are begun. A maximum 24 hours of hold time will be allowed for each failure.

3) ***Total time*** – The time elapsed from the start of the availability test until the end of the availability test.

4) ***Test time*** – The time elapsed from the start of the availability test until the end of the availability test, excluding hold time, i.e., *Test_time = Total_time – Hold_time.*

22.11.3 Duration and Criteria for Passing

The minimum duration of the availability test shall be 1,500 consecutive hours of test time.

To establish that all failures have been satisfactorily repaired prior to the end of the availability test, no downtime, intermittent (hold time) failures, or more than one un-commanded failover shall have occurred within 200 hours of the test's conclusion. The test shall be extended, if necessary, to satisfy this requirement.

After 1,500 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 = [(Test_time – Down_time)/Test_time] x 100%

If the system availability requirements presented in Clause 14.8, System Availability, have not been met, the test shall continue until the specified availability is achieved. Alternatively, at the Authority's discretion, the test may be restarted.

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 Clause 14.8.2, Availability Requirements. If one or more devices do not meet the requirements, the test shall be extended until the Authority and the Contractor mutually agree that corrective action has been completed for those devices. Corrective action shall include all necessary procedures to test and verify proper operation to the Authority's satisfaction.

23. Training

The Contractor shall prepare and deliver a comprehensive training program on the operation and maintenance of the TDMS. This shall include hands-on training associated with Authority use of the Development System in its early deliverable configuration (refer to Clause 13).

Software training shall teach the Authority the skills required for TDMS maintenance and expansion and for the preparation and integration of new functions. This training shall cover the theory of design and operation, use, maintenance, and installation of upgrades or new releases of these software products.

Hardware training shall qualify the Authority to perform routine preventive maintenance and perform diagnostic tests on the processors and their peripheral equipment including firewalls, routers, video walls, and communications equipment.

23.1 General

23.1.1 Course Styles

The Authority 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 only. A copy of any video cassette, CAI program, or CBT program used in training shall be provided to the Authority as part of the training documents.

23.1.2 Recording of Courses

The Authority shall be permitted to make video and audio recordings of all training classes. The Authority will use these recordings solely for internal instruction purposes and will not release the recordings to third parties.

23.2 Training Documents

The Contractor shall prepare a training plan in cooperation with the Authority. The Contractor shall also be responsible for the preparation and production of all course material. Training documents shall be subject to the review and approval process of Clause 21.3, Documentation Review and Approval.

23.2.1 Training Plan

The training plan shall support the TDMS implementation schedule. A logical sequence of courses shall be arranged, so that training on base system elements (such as the hardware platform, operating system, languages, database, and displays) is given before the training for specific TDMS elements such as applications. The training program shall consider the knowledge required by members of the Authority's project team in order to participate in the project.

The training plan shall list each course to be taken, the dates for the course, and the expected number of trainees to attend. The plan shall reference the course description documents described below.

Training shall be scheduled to minimize the loss of knowledge through lack of use, i.e., training shall be scheduled so that there will not be long periods of time between training and use of the training.

It is the Authority's preference that all training, except for Dispatcher Training, be completed prior to the start of factory acceptance testing.

23.2.2 Course Descriptions

Course descriptions shall be included with the training plan to provide the following information for each course included in the training plan:

1) The course name (and number if applicable)

2) A brief description of the course

3) A description of the intended audience for the course

4) A description of the relation of the course to others in the training plan

5) The duration of the course

6) A breakdown of the course schedule, identifying classroom, laboratory, and hands-on periods

7) A list of the training materials to be supplied

8) A list of reference material to be used in the course

9) A list of any prerequisite training or experience expected of the trainees.

At the Authority's request, the Contractor shall provide a description of all courses offered by the Contractor and its subcontractors.

23.2.3 Course Material

The Contractor shall provide all necessary training materials including course manuals and reference materials. Each trainee shall receive individual copies of the training materials. Additional sets shall be provided, one for the Authority's archives at headquarters and one for each of the project’s control centers. Class materials, including documents sent before the training classes and class handouts, shall become the property of the Authority.

The Authority prefers that all course material be transmitted to the trainees at least two weeks prior to the course.

23.3 Instructor Qualifications

Course instructors shall have demonstrated technical competence in the subject and previous instructing experience. The Authority prefers instructors who specialize in course presentation as opposed to hardware or software developers who only occasionally present courses. However, for TDMS elements produced specifically for this Contract, the Contractor may use the developer as the instructor. The developer shall use appropriate training staff as resources when developing the training course and materials.

Where practical, subcontractors shall deliver training on their products directly. However, the Contractor shall remain responsible for selecting these courses, coordinating their delivery, and ensuring that all training objectives are met.

In addition to the above, if the course instructor is not proficient in the Thai language, the Authority would prefer that the Contractor also provide an interpreter, with relevant technical background, to help the instructor deliver his presentation as efficiently and effectively as possible.

23.4 Training Curriculum

The training curriculum presented in this clause is intended to describe the contents of the training when viewed in its entirety. The subjects covered by individual courses may differ if the overall objectives are satisfied.

23.4.1 TDMS Seminar

Two types of TDMS Seminar shall be given, referred to herein as the TDMS Seminar for Technical Support Group and the TDMS Seminar for Executives.

23.4.1.1 TDMS Seminar for Technical Support Group

This TDMS Seminar shall be the very first course in the training sequence. The seminar shall constitute an introductory class for Authority personnel who typically will participate in the project as members of the project team or as managers with a special interest in the project. Most of the attendees will also attend the Contractor's subsequent training courses. Thus, the TDMS Seminar for Technical Support Group shall present not only a general overview of the project, but also details related to understanding the TDMS architecture, its functions and technology, the project schedule and its various phases, how the project will be implemented, the role to be played by Authority personnel, and the training they will receive.

23.4.1.2 TDMS Seminar for Executives

In contrast to the TDMS Seminar for Technical Support Group, the TDMS Seminar for Executives shall not be scheduled until the TDMS has been accepted by the Authority and the Functional Guarantee Certificates have been issued. The seminar shall provide ample opportunity for free interchange between the Contractor and Authority personnel. Many of the attendees will include managers concerned with system operations at the Authority's data centers as well as control centers. Thus, the seminar shall provide a high-level overview of the TDMS functions and technology with emphasis on the project's objectives, the results achieved, and how the TDMS master stations should be operated and managed.

23.4.2 Database and Display Building

The database and display building courses shall be scheduled to coincide with the delivery of the Development System (DS). The courses shall teach trainees how to prepare the input data to define the TDMS operating environment, to build the TDMS database and displays, and to prepare the database administrator to maintain and modify the database and its structures. The courses shall include classroom instruction reinforced by hands-on-training in the form of workshops making full use of the DS facilities.

The topics to be covered shall include:

1) How to set up a TDMS database and display building environment.

2) How to identify database fields, entries, records, tables and contexts.

3) How to structure data source table definitions.

4) How to build tables and arrays.

5) How to build application models, such as network analysis and load forecast models.

6) How to build displays.

7) How to perform database maintenance.

8) How to generate the database from source materials including data imported from the Authority's GIS.

9) How to prepare data to be sent to other computer systems such as the GIS.

10) How to maintain symbol libraries and other display constructs.

Once these topics have been covered in a classroom environment, the required workshops shall be used to bridge the gap between understanding the conceptual and theoretical aspects of building databases and displays and being able to build such databases and displays. These workshops shall utilize the Authority's actual data, displays, and models to ensure that the Authority is properly engaged in database and display building activities. Thus, as a minimum, the workshops centered on hands-on training using the Development System shall include:

1) The most effective and expeditious way to set up databases that reflect the need to collect data and send commands to the field device interfaces and to import and export data with respect to other computer systems. This shall include:

    a) Mapping data in the external data sources to the TDMS.

    b) Identifying all additional data that is not in the data sources, but needs to be collected for input to the TDMS.

    c) Procedures to transmit data between the DS and the TDMS staged on the factory floor.

2) Display building design issues.

3) Discussion of application-specific modeling techniques and related database requirements.

4) Discussions of the different approaches to storing and retrieving historical data.

5) Development of a program for data and display development activities.

6) SCADA database generation and conversion.

7) Database development to support functions such as those comprising the power system applications including concepts related to function execution in real-time, study, and simulation mode.

8) Information Management database development.

9) Display generation.

At the end of the Database and Display Building course, the trainees shall be able to:

1) Understand the Contractor's terminology

2) Perform data entry and data validation

3) Produce database reports

4) Identify the types of data needed to model the Authority's power system

5) Describe the functional capabilities of the Contractor's graphical display editors

6) Create simple images with basic figure types

7) Create new symbols

8) Describe the use of icons

9) Define the visual attributes of symbols on one lines to show changing data values

10) Describe the use of color on one-lines

11) Construct the static parts of a one-line display

12) Design displays that use multiple view capabilities to change the amount of detail presented

13) Design displays to emphasize important information

14) Describe the application of full graphics technology to the user interface

15) Create a new data source and install it in the system, including:

    a) Describe the data requirements of the data source

    b) Describe the data addresses

    c) Build the linkage between the data source and these addresses

    d) Create, for the data source, a complete set of displays

    e) Build the linkage between the data addresses and multiple displays using symbols, colors, etc.

f) Build linkages between the schematic and geographical overview displays

g) Create poke points for display selection.

23.4.3 IS&R Management

These courses shall be designed to train Authority personnel in management and use of the IS&R capabilities of the TDMS, including selections of items to be archived, calculations associated with historical data, and report building features. These courses shall be especially oriented for those of the Authority personnel who develop and maintain displays, reports, and calculations relating to IS&R and for those Authority personnel who maintain the TDMS as an enterprise-wide resource.

At the end of these courses, as a minimum, trainees shall be able to:

1) Create and maintain the IS&R database.

2) Understand SQL features and functions.

3) Construct SQL queries to retrieve, sort, summarize, and change data.

4) Develop strategies for writing efficient applications.

5) Define and develop interfaces to systems such as the Web servers.

6) Prepare web pages for use by the Web server.

7) How to create and maintain reports using the TDMS facilities.

23.4.4 System Administration and Programming

The System Administration and Programming course shall consist of several components to train Authority personnel, as software engineers, to perform all system administration tasks as well as to maintain the system from both an administration and detailed programming perspective. These components are described in the following sub-clauses.

23.4.4.1 Administration at System Level

This component of the System Administration and Programming course shall familiarize the trainees with the procedures necessary to operate the system as an integrated entity, to recognize and respond to system malfunctions, and to perform system level maintenance functions. Thus, the trainees shall be able to:

1) Start up and shut down the TDMS and its components

2) Switch functions to backup equipment

3) Take equipment out of service

4) Restore equipment to service

5) Interpret and react to messages generated by error-monitoring functions

6) Test field device interface and communication links

7) Implement procedures for installing new or modified applications for operations use

8) Use procedures for altering and replacing the operations database

9) Identify procedures for using diagnostics

10) Describe the backup functions required for normal maintenance

11) Use the system's procedures to generate the TDMS from source code or distribution media.

23.4.4.2 Administration at Operating System Level

This component of the System Administration and Programming course shall prepare the trainees to manage and maintain the TDMS at the operating system level so that, as a minimum, the trainees shall be able to:

1) Manage and maintain the system administration database and files

2) Manage and administer networks

3) Shutdown and restart the TDMS from different media, such as disk, tape, CD-ROM, and over the network

4) Backup and restore all programs and data

5) Add processors and peripherals to the TDMS

6) Add users to the TDMS

7) Update the operating system software

8) Access Contractor and subcontractor system level programming interfaces to facilitate the development of software by the Authority.

23.4.4.3 Programming in TDMS Software Environment

In addition to the above, the System Administration and Programming course shall instruct the trainee on the skills needed to program in the TDMS software environment and, from this perspective, be able to maintain, expand, or add new functions to the TDMS. Thus, as a minimum, the trainees shall be able to:

1) Plan the implementation of a new software function

2) Describe the directory structure and locate applications and all supporting functions and software structures

3) Design and implement program data structures

4) Add new attributes to existing data structures

5) Write and test programs

6) Use Contractor and subcontractor-provided programming interfaces

7) Configure the failover and restart functions for Contractor and any Authority-provided software

8) Generate error messages

9) Use the trace and debug utilities

10) Extract code and check code using the source code utility

11) Describe the inter-program communications process.

23.4.5 Cyber Security Measures

This course shall train Authority personnel so that they fully understand the cyber security measures that the Contractor has included as part of the TDMS configuration. As a minimum, this shall include training with respect to:

1) Internationally recognized cyber security standards.

2) How the TDMS cyber security measures relate to these standards.

3) How the cyber security measures need to be administered and utilized.

4) Details governing the system's secure logon features.

5) The security features associated with secure ICCP and DNP 3.0.

6) What steps should be taken in the event TDMS security is compromised.

Within this context, specific training related to the various security perimeters of the TDMS shall be provided including the rules and operational restrictions that apply to the TDMS Demilitarized Zone (DMZ) and to others such as those delineated, for example, by the firewalls comprising the TDMS configuration.

23.4.6 Communications Software

The Contractor shall provide training on the communications between data sources, the communications network software used by the TDMS within the context of its local area networks, and on the interfaces or communications links with external subsystems and networks. Training shall be provided for both Contractor and subcontractor supplied software and communications products.

At the end of this course, participants shall be able to:

1) Understand the basic communications theory used by the TDMS

2) Understand the communications design and implementation of the TDMS

3) Understand the protocol implementation

4) Install, startup, and test the initial configuration

5) Expand the communications

6) Perform diagnostics and maintenance procedures

7) Install communication upgrades.

23.4.7 Application Software

The Contractor shall provide training on application software. Each application course shall be organized to be responsive to the Authority's specific requirements and shall be regarded as an extension to the standard courses that are provided. Each course shall cover the following topics:

1) Functional design of the specific application program (using the approved functional specifications and displays as text)

2) Algorithms and models used by the application program

3) Programming techniques for the algorithms

4) Software implementation aspects, including each module's calling parameters and its interfaces with other modules as determined by these parameters and the data flags described

5) Database implementation aspects, including those portions of the database used by an application relative to content, structure, meaning, origin, and usage

6) Application program command language structure and common techniques

7) Application program procedures, including a review of standard procedures used to modify source code and compile, load, and install programs.

The design specifications and the user manuals prepared for the TDMS shall be used as course text where applicable.

23.4.8 DAC Simulator Course

This course shall cover the operation of the portable DAC Simulators that Authority personnel and others, such as the field device interface contractor’s personnel, will use to ensure the field device interfaces provided under separate DDIP contracts are ready for operation with the TDMS. After this course, trainees shall be able to:

1) Use the DAC Simulator to acquire data from each type of field device interface.

2) Verify the correct mapping of all data source points to the DAC database.

3) Use the DAC Simulator to verify that control commands sent to each type of field device interface are mapped correctly.

4) Identify mapping problems and take whatever action may be necessary to correct these problems.

5) Use all diagnostic and troubleshooting capabilities provided by the DAC Simulator with respect to maintaining field device interfaces, including the down loading of configuration and parameter information.

23.4.9 Hardware Maintenance

This course shall teach the trainees the basic theory and operation of each hardware component comprising the TDMS and the essential knowledge and skills required to maintain and troubleshoot to the level of field replaceable modules. Emphasis shall be placed on the practical application of diagnostic software tools as well as any special tools and instruments used in performing both preventive and maintenance activities.

The course shall include entry-level training in the use of operating system skills, an introduction to the critical directories and files that drive the operating system, and a discussion of the related software, system boot process, networking concepts, and terminology for computer hardware.

The level of training shall be commensurate with the Authority's intent to keep the TDMS in continuous working order using its own staff following acceptance of the system. The training shall be provided on actual TDMS equipment or on similarly configured systems. Most of the training time shall be spent in hands-on exposure to all TDMS hardware.

The course shall be designed for the hardware maintenance technician, who has computer maintenance experience, but no detailed knowledge of the TDMS hardware. At the end of this course, the trainees shall be able to:

1) Install, configure, diagnose, and verify the proper operation of processors, workstations and PCs, communication interfaces, and all TDMS peripheral equipment.

2) Troubleshoot malfunctions introduced into the system using all available diagnostic tools.

3) Perform TDMS hardware fault isolation and repair.

4) Understand the general features, characteristics, and the trouble shooting issues for all hardware supplied by the Contractor including the video wall equipment.

23.4.10 On-the-Job Training

To supplement formal training, the Authority will locate staff at the TDMS factory site as well as at Authority project sites to participate in On-the-Job training (OJT). In this respect, the Contractor's proposal shall have described a comprehensive OJT program where the main objective is to train Authority personnel in system integration and development, hardware maintenance, database and display generation (including system data import and export capabilities), system security, and all details concerning the TDMS software (such as those associated with maintenance and integration of the SCADA functions and power system applications). The proposed program shall include the recommended number and types of OJT specialists, all prerequisites, the schedule for completing the OJT program, and any other necessary details. On-the-job training shall apply to the Development System and DAC Simulators as well as the TDMS main platform and remote workstations. Within this context, the OJT program shall also include detailed exposure to all aspects of the TDMS security features.

During this training, the Authority's personnel may provide system implementation support such as clarifying Authority requirements and related issues and helping to develop TDMS interfaces with external systems (e.g., Authority OMS, GIS, MDMS, AMS, and EGAT's EMS). Their participation and performance shall in no way relieve the Contractor from any contractual obligation.

The OJT staff will attend training courses scheduled to promote early involvement in the implementation work. They will spend at least 75% of their time at Contractor facilities during development of the system through factory acceptance testing. They will also be involved in system integration and system performance testing and be trained to utilize the Contractor's standard software development, documentation, and quality assurance including system security practices.

The Contractor shall utilize the OJT staff as working members of the project team. They will begin assignments at a time recommended by the Contractor and approved by the Authority. Work assignments by the Contractor shall be subject to Authority approval. The Contractor shall schedule the work assignments to normal working hours and in such a way that no more than 50% of their time shall be spent on these work assignments. The remaining time shall be based on other activities such as training, unstructured testing, and project management (such as reporting progress to the Authority's project manager and helping to resolve any specific issue that may arise). The Contractor shall retain responsibility for all work assigned to or completed by the Authority's OJT staff.

23.4.11 Dispatcher Training

The objective of this course is to train Authority staff in preparation for development and presentation of Dispatcher training courses by the Authority. The Dispatcher Training course shall include:

1) A system overview that presents the TDMS configuration, application, capability, and performance concepts.

2) General operating procedures that cover basic user interface features, display and report capabilities, log-on steps, areas of responsibility, user access restrictions, error messages, etc.

3) Use of applications in real-time, study, and simulation modes under a full range of typical operating conditions, including purpose, theory of operation, and the user interface features that support each application.

4) Equipment handling such as minor system maintenance activities that do not require a technician.

5) Verification that the information in the TDMS user's manual is valid.

23.5 Number of Attendees and Location

The maximum number of expected attendees for each training course and the desired course locations are listed in Exhibit 23-1. For some courses, a single cycle will not be enough due to the large numbers of attendees and the problem of scheduling for such large numbers. Therefore, as indicated in Exhibit 23-1, some courses shall be repeated.

Exhibit 23-1: Course Attendants and Preferred Locations

Course Names	Attendees per Cycle	Number of Cycles	Locations	Estimated Working Days per Cycle
TDMS Seminar for Executives (see note below)	100	1	Authority site	1
TDMS Seminar for Technical Support Group	40	2	Authority site	1
Database and Display Building	30	2	Authority site	5
Information Management	30	1	Authority site	5
System Administration and Programming	30	1	Authority site	5
Cyber Security Measures	30	1	Authority site	5
Communications Software	30	1	Authority site	5
Application Software	30	1	Authority site	5
DAC Simulator	30	2	Authority site	3
Hardware Maintenance	30	1	Authority site	5
Dispatcher Training	10	13	Authority site	5

Note: The TDMS Seminar for Executives shall not be given until the Authority has issued the Functional Guarantee Certificate (FGC) for the TDMS.

With respect to On-the-Job training, the Authority's provisional estimates for the number and types of specialists who will participate in this training are listed in Exhibit 23-2. Final details of the OJT program shall be negotiated and agreed upon prior to contract signing.

The Authority will be responsible for attendee travel and living costs with respect to those courses in Thailand that are away from the attendees assigned offices. For training given at Contractor or other facilities overseas, the Authority will be responsible for international airfares and per diems covering meals. Otherwise, while Authority staff is receiving training overseas (as in the OJT program), the Contractor shall be responsible for attendee local transportation costs and accommodation.

Exhibit 23-2: On-the-Job Training Specialists and Locations

OJT Specialists	Attendees per Cycle	Number of Cycles	Locations	Estimated Months per Cycle
System Integration & Development Specialists (including Cyber Security)	8	2	DMS Factory & Authority sites	3
Hardware Specialists	8	2	DMS Factory & Authority sites	1
Database & Display Specialists (including data exchange with GIS, OMS, etc.)	8	2	DMS Factory & Authority sites	2
SCADA & Application Specialists	8	2	DMS Factory & Authority sites	3

23.6 Training Schedule

The schedules for all formal training courses (including on-the-job training) shall be included in the project's detailed implementation schedule to be submitted by the Contractor for Authority approval in accordance with Clause 24.5.5 of these Technical Specifications.

23.7 No Additional Charges

The Contractor shall be responsible for the cost of additional training courses, and the travel and living expenses of trainees attending these courses, where the need for such training is attributed to any of the following conditions:

1) Significant delays in the project schedule caused by the Contractor.

2) Inadequate or poor-quality training that fails to meet the Authority's requirements for quality, content, or timeliness.

3) Changes to any hardware or software deemed necessary during the project to meet the requirements of the contract.

4) Any change in the scope of the contract, unless the cost of the additional training is included in the cost of the change.

24. Project Implementation

This clause specifies project implementation requirements that have not been covered elsewhere in these Technical Specifications or require further elaboration. They include requirements concerned with

project management, project tracking, and project documents. Other requirements are covered such as those that relate to system testing, shipment, cutover, commissioning, and maintenance. Project security initiatives are also addressed. Within this context, Contractor implementation responsibilities shall include all elements of the project that concern proper management and timely execution of the TDMS.

24.1 Consultants

The Authority expects to retain the services of a consultant for assistance with the project. Consultants shall be part of the Authority' staff and shall be given access to all project documentation and information and shall be permitted to participate in project meetings, testing, and all other project activities.

24.2 Third-Party Software

Where any Contractor-provided applications software or software modules developed by a third-party are integrated into the TDMS, the Contractor shall be responsible for integrating, testing, and meeting the functional, security, and performance requirements of this software in the TDMS environment.

24.3 Project Organization

The primary points of contact between the Authority and the Contractor shall be their respective project managers.

24.3.1 Authority's Project Manager

The Authority's project manager shall be responsible for representing the Authority's interests throughout the project. The Authority's project manager may, from time to time, authorize other staff to act in this regard for specific tasks. The project manager may also change such assignments from time to time. Such actions will be submitted to the Contractor in writing.

All formal correspondence with the Authority shall be addressed to the Authority's project manager.

24.3.2 Contractor's Project Manager and Project Personnel

The Contractor shall designate a project manager who shall be responsible for the co-ordination of all project work and for the communications between the Contractor and the Authority. Except for conditions outside the control of the Contractor, the Contractor's project manager shall not be removed or replaced without the approval of the Authority.

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 TDMS. 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 DDIP.

The Contractor shall inform the Authority of any pending or possible changes in the use or status of all Contractor project personnel. Any changes to Contractor staff, including work assignments and participation level, shall be announced as soon as practical and shall be subject to the Authority's

approval. The Authority shall have the right to have any Contractor staff removed from the project for due cause.

24.3.3 Authority Office at TDMS Factory

The Contractor shall make available office facilities for use by Authority personnel when working or otherwise visiting the TDMS factory during project implementation. Office space, furniture, and reasonable office services such as Internet access, telephone, copying, printing, mail and courier services, access to meeting rooms, and secretarial assistance shall be provided.

These offices shall be contiguously located and, as a minimum, shall be kept available for the exclusive use of the Authority through completion of all TDMS factory tests. The offices shall allow confidential documents, personal effects, and other materials to be stored securely.

24.4 Project Tracking System

The Contractor shall be responsible for providing a convenient project tracking system. Thus, in addition to the formal project correspondence and monthly progress reports specified in Clause 24.5 below, the Contractor shall set up and maintain a project web site that will allow Authority and Contractor personnel to both access and post information in the form of transmittals, reports, and other documents related to tracking and recording the status of the project and its numerous activities on a day-to-day basis.

Project monitoring via the web site shall include a convenient means of reviewing Contractor comparisons of completed tasks versus scheduled tasks and estimates of the required effort to complete the remaining tasks. On this basis, using the web site, the Contractor shall also present frequently updated schedules to reflect the Contractor’s best effort at projecting progress of all major tasks yet to be accomplished. To support such presentations, in the monthly progress reports as well as on the web site, the Contractor shall make use of a commercially available project management application such as Microsoft Project.

Within the context above, the web site shall include for example:

1) Both formal and informal project transmittals.

2) Project documents including review comments and subsequently updated documents in accordance with document review and approval procedures.

3) Summaries of issues raised and subsequent resolutions.

4) Listings of open and closed action items with corresponding dates.

5) Meeting and test schedules.

6) Records of meetings held with associated meeting minutes.

7) Records corresponding to completed events, tasks, and milestones such as those that relate to:

a) Demonstrations, testing, installations, commissioning, and inspections.

b) Deliveries of documentation, hardware, and software (including software licenses).

c) Completion of training courses.

8) Records of open and closed variances.

9) Updates related to the progress of TDMS database, display, and report preparation activities.

10) Records of Contractor invoices including dates and amounts when payments were requested along with dates and amounts when payments were received.

11) Details related to changes of scope such as descriptions and status.

All features of the project tracking system, including any software products that may be available to enhance both the efficiency and content of the web site from an overall project management perspective, shall have been described in the Contractor's proposal. The web site (at least in preliminary form) shall, be up and running no longer than one month after Contract signing date.

24.5 Project Documents

Project documents shall include the specific documents presented in Exhibit 24-1. These documents and their delivery requirements are described in the following sub-clauses.

Exhibit 24-1: Project Documents

Document	Reference Clause
Documentation Plan	Clause 24.5.1
Project Progress Report	Clause 24.5.2
Project Meetings, Agendas, and Minutes	Clause 24.5.3
Project Correspondence	Clause 24.5.4
Detailed Implementation Schedule	Clause 24.5.5
Site Installation and Cutover Plan	Clause 24.5.6
Test Documents	Clause 22.4
Training Documents	Clause 23.2

24.5.1 Documentation Plan

A documentation plan shall be submitted to the Authority twenty (20) working days after Contract award. The documentation plan shall describe, in detail, the Contractor's plan for the submittal of all subsequent TDMS documentation.

It is expected that certain major documents, such as the detailed hardware and software design documentation, will consist of a series of submittals made over a period of time. The documentation

plan shall address this by including a detailed list for all individual documentation submittals. This list shall include, but shall not be limited to the following information for each document:

1) Document name.

2) Document number.

3) Document type (such as, functional design, detailed design, listing, or user guide).

4) Estimated and actual date of submittal.

5) Document status (such as, submitted for review, submitted for approval, returned for correction, or approved.).

The plan, including the list above, shall serve as a checklist throughout the project and shall be revised and resubmitted by the Contractor as necessary.

Documents shall be submitted in a sequence that allows the Authority to access all the information necessary for reviewing or approving a document at the time of its submittal. Documentation shall be submitted in a manner that allows for a reasonably paced review effort, but also allows for timely coordination with project activities that need to make use of the documentation. The documentation plan shall be subject to Authority approval.

24.5.2 Project Progress Reports

A project progress report shall be prepared by the Contractor and sent to the Authority each month through the start of the warranty period. The report shall be submitted to the Authority's project manager no later than the 10th calendar day of each month. The report shall cover all elements of the project from the start of the Contract through the last working day of the month.

The progress report shall include a general assessment of progress on the project. This assessment shall reference the latest implementation schedule, which shall be included in the report. The schedule shall show the baseline and the current schedule, progress on individual tasks, and the forecasted completion dates for upcoming tasks and the entire project. Updated training and documentation plans shall be included.

The report shall include an explanation of existing and forecast schedule variances, the cause or source of the variance, alternatives considered, solutions adopted or recommended, and the outcome achieved or anticipated. The report shall note the needed delivery date of Authority-furnished information. The Contractor shall be responsible for any schedule delays due to insufficient notification to the Authority of the need for such information.

The report shall identify unresolved Contract and technical issues. This shall include a description of the item and the current due date, the consequences of any delay in resolution, and any recommendations pertinent to the decision process.

The report shall also include the following items:

1) A list of action items, including the following information:

   a) Action item number.

   b) Date the item was opened.

   c) References to the originating transmittal and any reference documents.

   d) Action item status (open, closed).

   e) Resolution due date.

   f) Responsible organization or person.

   g) Description of the action required.

   h) Date of action completion (when each item is closed).

   i) References to transmittals or other documents recording the resolution.

2) Correspondence logs, one for transmittals to the Authority from the Contractor and one for transmittals to the Contractor from the Authority. Each log shall have the following information for each transmittal:

   a) Transmittal number.

   b) Date of transmission (not date written).

   c) Date received.

   d) Subject of the transmittal.

   e) Identification of any action items addressed by the transmittal.

   f) List of any documents attached to the transmittal.

3) A Contract change log containing the following information for each required change in any requirement:

   a) An identifying number.

   b) References to documentation of the change.

   c) A list of the affected Contract sections.

   d) A concise summary of the change.

   e) Cost information.

4) Status of training program.

24.5.3 Project Meetings, Agendas, and Meeting Minutes

Project meetings shall be held to review project progress, to ensure correct interpretation of the Contract, to review technical and commercial issues, and to maintain co-ordination between the Authority and Contractor. The Contractor's project manager shall prepare a meeting agenda in time for review by the Authority, i.e., under normal circumstances, at least one week before each meeting. The meetings shall be categorized and scheduled as follows:

1) ***Formal Progress Review Meetings*** – As a minimum, these meetings shall be attended by the Authority and Contractor project managers supported by their key project team leaders. The meetings shall take place at Authority offices at least every three (3) months to review project progress and to resolve any technical or commercial issue that may be impeding progress in accordance with the approved schedule.

2) ***Project Team Meetings*** – These meetings shall be attended by relevant members of the Authority and Contractor project teams on an as needed basis to manage the project's day-to-day implementation activities. Typical meeting topics shall include clarifying Authority requirements, reviewing and agreeing on work flow procedures, resolving design and engineering issues, handling change orders, coordinating and scheduling project team activities, etc. Most of these meetings shall take place at Authority offices.

The Contractor shall prepare the minutes of each meeting and submit them for review within one (1) week following the meeting. Both the Authority and the Contractor shall review and approve the minutes. The approved minutes shall be considered binding agreements, subject to concordance with the Contract. Where the approved minutes conflict with the Contract, either the minutes shall be revised or a change order to the Contract shall be generated. Where the minutes of a meeting conflict with the approved minutes of a previous meeting, the conflict shall be documented in the later minutes and these subsequently approved minutes shall have precedence.

24.5.4 Project Correspondence

All requests and transfers of information between the parties shall be made in writing, and shall be documented with letters of transmittal. All correspondence from each party shall be dated (with the date of transmittal, not the date of writing) and uniquely numbered. With the exception of the meeting minutes, each letter or other project correspondence shall be limited to a single topic to simplify correspondence management.

Correspondence may be exchanged by electronic mail (e-mail). Such correspondence, including any agreements construed therein, shall not become official until it has been followed up by formal "hardcopy" correspondence. In this respect, a printed copy of an e-mail attached to a transmittal cover sheet is not acceptable as formal correspondence.

All project management documentation, such as correspondence, memos, meeting minutes, and monthly progress reports, shall be produced using the Microsoft Office productivity suite. A mutually agreeable file numbering scheme shall be developed and used to minimize file storage and retrieval efforts.

24.5.5 Detailed Implementation Schedule

The Contractor shall submit for the Authority's approval a detailed implementation schedule. This shall describe all the project activities of both the Contractor and Authority. As a minimum, the schedule shall include the following:

1) Payment milestones.
2) TDMS hardware procurement, integration, and testing.
3) Training courses and dates.
4) Submittal dates, review cycles, and acceptance dates for the hardware, software, and interface requirement documents.
5) Testing and delivery dates for Development System (DS) and DAC Simulators.
6) Delivery dates for Authority-furnished data, interface equipment, etc.
7) Software development on a per-function or per-interface basis.
8) Software unit testing.
9) Subsystem integration and testing.
10) Interface testing.
11) Preparation of test plans and procedures.
12) TDMS factory testing (both Pre-FAT and FAT).
13) Variance correction and retest.
14) TDMS disassembly, delivery, installation, and cutover.
15) Site testing.
16) Project commissioning activities.
17) Final system and user documentation.

24.5.6 Site Installation and Cutover Plan

In consultation with the Authority, the Contractor shall develop a comprehensive site installation and cutover plan detailing the steps that will be taken:

1) To install and unit test the TDMS equipment at the Authority's data centers and control centers while minimizing interruption of real-time power system operations by the Authority using existing SCADA/EMS/DMS facilities. This shall include recommendations with respect to

movement and placement of both new and existing equipment whether on a temporary or permanent basis.

2) To begin and complete testing of the integrated TDMS in parallel with the existing facilities from the perspective of establishing communications and correct interoperation with all substation and feeder field device interfaces. This shall include interoperation with EGAT's SCADA/EMS as well as integration with Authority enterprise systems such as the GIS and startup, for example, of web services in support of Authority operations and non-operations personnel. Testing shall also ensure the TDMS databases are accurate, fully up to date, and capable of supporting the TDMS applications.

3) To complete transition from using existing SCADA/EMS/DMS facilities to using the integrated TDMS for normal every-day real-time operations. This shall include utilization of a listening mode with the existing facilities. It shall also include final placement of new equipment along with the dismantling and removal of all unnecessary existing equipment.

24.6 Project Security Initiatives

The Contractor's project manager shall be responsible for ensuring that the Contractor and the Contractor's staff complies with all required TDMS security requirements and provisions for the life of the project.

24.6.1 Project Security Documentation

The Contractor 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 systems, and to protect the reliability of these systems.

24.6.2 Security Preparation

Prior to TDMS commissioning, the Contractor 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. Removed items include, but are not limited to: developer user accounts in production systems, testing access permissions to processors, data and applications, test scripts, and test data.

All updates to operating system and application software addressing cyber security issues shall be installed prior to system commissioning. 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. Software shall immediately be placed under source code control after scanning.

The Contractor and Authority 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.

24.6.3 General Security Considerations

The following clauses describe the non-technical security requirements to be met. These security requirements, based on standards such as NERC CIP-003 through CIP-009 (or equivalent), are in addition to the technical security requirements described elsewhere in these Technical Specifications.

24.6.4 Security Management Controls

The Contractor shall assist the Authority to classify information that the Authority will provide to support the project. On this basis, the Contractor shall establish, document, and use an Authority approved security policy governing access to this information. As a minimum, the resulting security policy document shall address access to procedures, critical asset inventories, maps, one-line diagrams, floor plans, equipment lists and layouts, configurations, databases, and application software, etc. The document shall identify measures that provide both electronic and physical protection for the sensitive information. When the Contractor no longer needs the information, all copies shall be returned to the Authority, or destroyed as specified by the Authority.

The Authority and Contractor shall protect all project data transmitted between Contractor and Authority sites and shall jointly determine the methods required to securely transmit this data. Experience in the secure transmission of project-related data shall have been included in the Contractor's proposal.

The Contractor shall provide the Authority with a documented procedure for accessing the project's systems and equipment while located at the Contractor's site. This process shall include a review and approval process to ensure that only authorized personnel (i.e., Contractor staff, sub-contractors, and suppliers) have access to these systems and equipment, including the Authority information associated with them. The Authority may request a review of the procedure and the list of authorized personnel at any reasonable time during the project.

Logical access to the systems by Contractor staff shall be limited to that required for the staff to perform their project duties, based on appropriate roles and responsibilities documented as part of the security policy.

The Contractor shall maintain a list of personnel who are responsible for authorizing access to the systems and equipment, identifying each by name, title, business telephone, and the list of systems, application functions, and equipment for which they are responsible.

24.6.5 Personnel and Training

All Contractor staff with access to the Authority's systems and equipment shall be trained in appropriate and applicable security practices. The Contractor shall provide copies of training materials to the Authority for review and approval. Based on its review of Contractor training materials, the Authority may request the addition of specific topics to the training required for those staff that will be given access to the Authority's systems and equipment. Training shall be conducted annually, with attendance records maintained for inspection by the Authority. Included in these training records shall be the date of training, lists indicating Contractor staff attendance, and a course syllabus.

Background monitoring shall be performed to a degree consistent with the access granted, and in accordance with national, state, provincial, and local laws. The Contractor shall indicate any provisions in collective bargaining unit agreements that preclude the implementation of any provision for background checks. The Contractor shall provide the Authority with a copy of the process and requirements used in performing background monitoring. With respect to key Contractor personnel, such as the project manager and his team leaders, the following minimum investigative scope is required:

1) Employee Reference Check.

2) Personal ID Verification.

3) Education/Professional Affiliation Verification.

The Contractor shall maintain records of background checks for 5 years and shall provide evidence of background checks to the Authority upon demand.

The Contractor shall communicate any personnel changes to the Authority and provide evidence of background checks and proper authorization and training for additions to the project staff. Change in assignment shall be communicated to the Authority within 7 calendar days of the change, or 24 hours if this involves removal for due cause.

The Contractor shall provide quarterly summaries of personnel assigned or authorized for access to the Authority systems and equipment for reconciliation with the Authority's records. The Authority and Contractor will investigate any inconsistencies jointly.

24.6.6 Electronic Security and Incident Reporting

The Contractor shall maintain a secure network for development of the Authority's TDMS and shall identify the electronic (logical) security provided while the TDMS is under the control of the Contractor at the Contractor's development site. This includes a description of the network access control features (e.g., firewall rule sets) used to limit or restrict unauthorized electronic access to the TDMS, or access to information and documentation about the Authority's TDMS or power system network, and to protect the Authority's TDMS from inadvertent and inappropriate use.

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. Summary reports of attempted and unauthorized access attempts shall be made available to the Authority at least monthly or more often if conditions warrant. The Authority shall be notified of all Electronic Security breaches or aggressive attacks of the Contractor's network and systems while the Authority's TDMS is under development at the Contractor's site, regardless of whether they were successful. The Contractor shall investigate the electronic security breach following established procedures, including applicable or required reporting to local law enforcement.

24.6.7 Physical Security and Incident Reporting

The Contractor shall identify the physical security provided to the Authority's systems and equipment while under the control of the Contractor at the Contractor's development site. This includes a description of building and floor access controls, controls to the "test floor", and provisions for securing access to the Authority's systems and equipment within the test floor environment. The physical security described shall include limiting access to information and documentation about the Authority's systems, including the power distribution networks, and protecting the Authority's systems and equipment from inadvertent and inappropriate use as well as from damage and theft. The Contractor shall provide monitoring and logging of physical access and provide appropriate records of access to the Authority upon reasonable request, or for cause.

24.6.8 Systems Security Management

When no longer needed, or at the end of the project, the Contractor shall destroy media such as paper documents and magnetic, electronic, and optical records containing sensitive or potentially sensitive information. Paper documents shall be shredded using a crosscut shredder (or equivalent). 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. CD-ROM disks must be physically destroyed rendering the data completely unreadable. The Contractor shall maintain business records of the destruction for inspection by the Authority. Cyber assets containing hard drives may be re-deployed within the Authority systems following hard drive content erasure, drive re-formatting, and drive re-loading with the new software or data as appropriate.

24.6.9 Recovery Plans for Critical Assets

The Contractor shall provide the Authority with recommendations pertaining to the development of a comprehensive procedure for the restoration of TDMS core functions and its full functionality following a catastrophic failure of the TDMS software or hardware.

24.7 Testing, Shipment, and Commissioning

The transition of activities from the implementation of the TDMS in the Contractor's facilities through testing, shipment, installation, cutover, and commissioning is crucial to the success of the project. This clause sets out the sequence of these activities and expands on the responsibilities of the Authority and the Contractor for these activities.

24.7.1 Factory Test Sequence

TDMS factory tests are described in Clause 22, Quality Assurance and Testing, along with conditions for test initiation and completion.

As a minimum, these tests include a preliminary factory test, a factory test, and a stability test. They shall be executed in the following sequence:

1) *Preliminary factory test (Pre-FAT)* – Successful completion of Pre-FAT is a pre-requisite for factory testing. This activity shall be scheduled as necessary to maintain the overall project schedule.

2) *Factory test (FAT)* – FAT, including the functional, performance, and unstructured tests, shall be started no sooner than two weeks after successful completion of Pre-FAT. The factory test schedule shall be set such that any member of the Authority's staff assigned to testing shall not be required to be at the Contractor's facility more than three consecutive weeks.

3) *Stability test* – The stability test shall be started immediately after successful completion of FAT.

4) *Cyber security audit* – The cyber security audit for the TDMS shall be performed immediately after successful completion of FAT on a non-interference basis with the stability test.

24.7.2 Authorization for Shipment

Acknowledgement of the successful completion of all factory tests related to the TDMS shall be deemed as authorization for the Contractor to ship the tested hardware and software to the Authority's site. Shipment will not be authorized until all major variances have been corrected to the Authority's satisfaction. However, the Contractor shall submit an official notice of intent to ship at least one month prior to completion of the factory test. The notice shall indicate the contents, names of all carriers, estimated shipping weight, size of shipment, insurance provisions, date scheduled to leave the factory, and estimated date and time of arrival at the Authority's facilities.

The Authority reserves the right to delay shipment if this notice is not given by the required time. Such delay shall be completely to the account of the Contractor – no schedule or cost relief will be granted.

24.7.3 Change Control

The Contractor shall establish and document a methodical process of change control and configuration management for identification, control, and reporting of any change to the project's software and hardware components both before and after shipment to Authority sites.

After the installation task (refer to Clause 24.7.4), all test plans, procedures, and results and any associated data shall be updated to reflect the current state of the delivered systems and equipment. The test plans and procedures shall serve as the basis for testing and verifying any changes that are implemented by the Contractor or Authority during the life of the project's systems and equipment.

24.7.4 Installation and Cutover

After project equipment is delivered to its assigned site, and the Authority confirms that it has been received in a complete and satisfactory manner, Contractor TDMS installation and cutover activities shall commence. The Contractor's Site Installation and Cutover Plan referenced in Clause 24.5.6 shall be followed. With Authority approval, however, allowance shall be made for any unforeseen circumstances requiring modifications to the plan.

The installation and cutover activities shall include updates including hardware upgrades to the on-site Development System (DS) and its integration as a fully operational component of the TDMS.

The Contractor shall be responsible for all installation and cutover activities. Authority personnel will supervise and assist where necessary. The Contractor shall meet with the Authority prior to delivery of the TDMS equipment to Authority sites to discuss the work necessary to install the TDMS equipment. If required, pre-installation visits to any of the various project sites shall be arranged. In addition, the Contractor shall become familiar with the Authority's labor and safety rules governing such installation work and shall design the installation work in accordance with these rules. As may be necessary, updates to the Site Installation and Cutover Plan shall be made.

Within this context, in coordination with other DDIP contractors concerned with the project's FDI and WRL communications scope of work, the Contractor shall be responsible for bringing the TDMS on-line and verifying its operational readiness in such a way that service interruptions are minimal. The Contractor shall also be responsible for supplying all necessary equipment, materials, and installation services to allow connections, including those with existing field device interfaces and other systems, to be individually switched and shared between the existing SCADA/EMS/DMS and new TDMS facilities during the transition period.

24.7.5 Commissioning

Commissioning in the form of the Site Acceptance Test (SAT), as described in Clause 22.10, shall demonstrate that the TDMS and all equipment is ready for commercial operation. The commissioning activities shall start immediately after successful completion of system installation and cutover as described in Clause 24.7.4. These activities shall include, but shall not be limited to checking that the on-site systems and equipment can provide the required functionality.

The Contractor shall be responsible for these tasks with support from the Authority where necessary. Via the site functional and performance test, the Contractor shall ensure that the TDMS is ready to meet the functional performance requirements associated with the guarantee test to be conducted by the Authority (refer to Clause 24.8).

After successful completion of these tasks, and before the TDMS is handed over to the Authority formally, i.e., for Authority commercial use of the system, the Contractor together with the Authority shall perform the site's cyber security audit (refer to Clause 22.9.6). In addition, the Contractor shall submit a full and complete TDMS commissioning report.

Successful completion of TDMS commissioning shall lead to Authority issue of a corresponding Provisional Acceptance Certificate (PAC).

24.8 TDMS Guarantee Test

Over and above commissioning, the TDMS shall be subject to a guarantee test. This test consists of two components as follows:

1) ***Functional Performance Capability*** – This test shall formally check the Contractor's functional guarantees with respect to the system's function execution times and user interface response times while running under typical operating conditions.

2) ***System Availability*** - This test shall formally check the Contractor's functional guarantees with respect to overall system availability, i.e., from the perspective of maintaining critical TDMS functionality while running under typical operating conditions.

Further details related to these components can be found elsewhere in the Technical Specifications (i.e., Clause 15, Capacity and Performance, and Clause 22, Quality Assurance and Testing).

The guarantee test shall be started as soon as possible after Contractor commissioning activities have been completed successfully. This requires formal Authority recognition that the TDMS is ready for commercial operation, i.e., the system's Provisional Acceptance Certificate shall have been issued. All major variances shall have been corrected prior to conducting the guarantee test. In addition, all other relevant prerequisites (Clause 22.6.1, Test Initiation) shall have been completed to the Authority's satisfaction.

The Authority shall be responsible for conducting the guarantee test with support from the Contractor. It will be conducted while the TDMS is in normal day-to-day operation. During the test period, the Authority will also monitor the general behavior of the system and report any variances that may be observed. The Contractor shall correct these variances as promptly as possible as part of the Contractor's system warranty obligations.

Satisfactory completion of either component of the guarantee test will lead to Authority issue of a corresponding Functional Guarantee Certificate. Certificates for both components must be issued prior to starting the TDMS warranty period.

24.9 System Maintenance

Once it is commissioned and handed-over for commercial operation, the TDMS shall be capable of being used and maintained by the Authority without requiring continual intervention or assistance by the Contractor. Within this context, the Authority's maintenance objective and related requirements during project implementation and during and after the TDMS warranty period are further described in the following sub-clauses.

24.9.1 Maintenance Objective

Due to the critical nature of its power system operations, the Authority's maintenance objective is to minimize system down time, i.e., to maximize the availability of the TDMS. To achieve this objective, the following criteria shall apply:

1) Maximum use of preventive maintenance procedures to avoid unnecessary down time.

2) Use of corrective maintenance procedures that minimize repair times especially during down times.

3) Provision of comprehensive and easy-to-use diagnostic software.

4) Provision of all equipment, test instruments, and spare parts necessary and sufficient to perform preventive and corrective maintenance.

5) Provision of comprehensive well-written maintenance and troubleshooting manuals.

6) Provision of all necessary and sufficient training so that all maintenance tasks can be accomplished as effectively and efficiently as possible.

24.9.2 Scope of Authority and Contractor System Maintenance

The Contractor shall be responsible for routine preventive and corrective maintenance of all Contractor-provided hardware and software until the Authority has accepted them and until their respective warranty periods begin. Subsequently, although responsibility for routine maintenance will pass to the Authority, the Contractor shall continue to perform all repair and variance correction work that may be necessary until the end of the warranty periods.

From the beginning of the project through completion of warranty, the Contractor shall supply all of the equipment, materials, tools, accessories, and spare parts necessary and sufficient to keep all systems and equipment in full and complete working order. The Authority does not intend to purchase such maintenance related elements during this period. Other elements such as printer paper, magnetic media, and cleaning materials, as also necessary for system and equipment maintenance, shall be supplied by the Contractor until the start of warranty. In all such respects, any element (including any spare part) that is necessary for maintenance, but is not specifically mentioned in these Technical Specifications, shall be taken into account and, from the Authority's perspective, shall be considered as included in the contract.

Routine maintenance shall follow procedures recommended by the computer system and equipment suppliers. In addition, as part of software maintenance from the beginning of the project until the end of warranty, the Contractor shall incorporate any software updates that become available periodically to improve, for example, the TDMS applications.

Throughout the warranty period, the Contractor's technical representatives shall be available to advise and assist the Authority's maintenance personnel. The Contractor shall also ensure that all facilities and component parts supplied by the Contractor remain free from defects in design, engineering, materials, and workmanship. Where there is a serious anomaly in the systems or equipment or their operating characteristics compared to the Authority's specified requirements, the Contractor shall take all necessary steps to overcome the anomaly as quickly and as efficiently as possible. This shall include the replacement of items on a permanent or temporary basis depending on whether the broken or damaged item can be repaired.

After the warranty period, the Contractor shall ensure that adequate spare parts remain readily available for Authority purchase for a period of at least ten (10) years.

24.9.3 Maintenance Reports

Throughout project implementation, including the warranty period, the Contractor shall keep a maintenance log for each system in which all inspections and repairs shall be recorded. These reports shall be available to the Authority upon request. In addition, every three (3) months, the Contractor shall send a report to the Authority summarizing all maintenance activities during the past three-month period.

24.9.4 Update and Information Services

The Authority is interested in keeping the TDMS and other software updated as the Contractor and OEMs make improvements and upgrades to their products. Within this context, the Contractor shall arrange to provide the Authority with such updates. This shall include keeping the Authority informed of all update and information services that are offered by any OEM and third-party software suppliers.

The update services shall be provided at the Contractor's expense for the duration of the respective warranty periods. After the Contractor's warranty expires, the arrangements made with the OEM and third-party software suppliers shall allow the Authority to initiate its own subscription to relevant OEM or third-party software supplier services. Likewise, on a continuing basis, the Authority shall have the option to subscribe to the update and information services offered by the Contractor.