Section -2, Chapter -4
SYSTEM SOFTWARE REQUIREMENTS

4.0 General

This section describes the characteristics of system software such as Operating system, RDBMS and support software (programming language compilers, database development and maintenance, display development, network services, report generation, diagnostics and backup utilities) to be provided by Contractor and the original software manufacturer as necessary to support the SCADA/DMS applications. This section also describes the standards to be followed for all supplied software. The contractor shall make use of common applications such as security, networking etc created under R-APDRP- IT infrastructure. However, it is necessary that functional, availability & performance aspects are met. Bidder shall assess the adequacy of software specified & if any additional software is required to meet all the requirements of the technical specifications, the same shall also be included in the offer.

4.1 Software Standards

All SCADA/DMS software provided by the Contractor, including the Operating system, RDBMS and support software, shall comply with the industry-accepted software standards produced by national and international organizations, such as ANSI, ISO, IEC, IEEE, ECMA in order to facilitate maintenance and enhancement of the SCADA/DMS systems being supplied. In areas where these organizations have not yet set standards, the software shall comply with those widely accepted de- facto standards put forth by industry consortiums, such as OSF and X/Open. The Contractor shall commit to meet the "open systems" objective promoted by industry standards groups by using software products that are based on open standards

.

4.1.1 Design and Coding Standards for SCADA/DMS applications

All SCADA/DMS applications shall be maintainable by employer using the supplied software utilities and documentation. The SCADA/DMS software design and coding standards shall also address the following:

(a) Expansion/ scalability: software shall be dimensioned to accommodate the ultimate size of SCADA/DMS system envisaged.

(b) Modularity: software shall be modular to minimize the time and complexity involved in making a change to a program.

(c) User-Directed Termination: Functions taking long execution times shall recognize and process user requests to abort the processing.

(d) Programming languages: The software shall be written using ISO or ANSI or ECMA standard programming languages like FORTRAN, C, C++,and SQL and for Unix based systems the APIs shall be POSIX-conforming.

(e) SOA architecture: Software shall conform to SOA.

(f) Enterprise service bus (ESB) : ESB based architecture is essential to enable interaction of applications from different product manufacturer , platforms etc.

(g) Portability & Interoperability: The software shall be designed for hardware independence and operation in a network environment that includes dissimilar hardware platforms to the extent possible. The use of system services software shall be built on Open standards

4.2 Operating System

The contractor shall use Unix /Linux / Microsoft Windows™ operating system servers. The servers based on of Unix O/s, shall generally comply with the evolving set of POSIX standards defined by IEEE.

4.3 Time and Calendar Maintenance

The SCADA/DMS system shall maintain Time and date for use by various software applications. The GPS based time receiver shall be used for synchronising the SCADA/DMS system time. All Servers and Operator workstation clocks shall be synchronised within the accuracy of +/-100 milliseconds. The SCADA/DMS system shall not be dependent on a particular server for time /calendar maintenance. . The SCADA/DMS shall include two redundant time and frequency standards. Failure of the online unit shall result in automatic switching to the redundant unit. The SCADA/DMS shall periodically check if the backup unit is operational and failure of either unit shall be alarmed.
The frequency reading shall be accessible by SCADA/DMS applications with three post-decimal digits resolution The system shall support communication protocols such as NTP and SNTP. The time and frequency standard unit shall support a common time code output format such as IRIG-B.

A surge protection system shall be included to prevent the time and frequency standard equipment from lightning.

4.4 Network Software

The network software for SCADA/DMS system shall include software for network communication, security and services.

4.4.1 Network Communication

Users and various applications shall be able to communicate within the SCADA/DMS local area network and operate as described in this Specification. The network communications software shall use a standard network protocol such as TCP/IP. The software shall link dissimilar hardware nodes, including local and remote workstations, application servers, communication servers, and various peripherals (such as printers) into a common data communication network allowing communications among these devices.

4.4.2 Network Security

A user authentication scheme consisting at least of a user identification and password shall be required for the user to request a connection to any network node.

4.4.3 Network services

The following network services shall be provided for the users of SCADA/DMS system:

(a) Network file management and transfer, for files containing text, data, and/or graphics information
(b) Network printing management
(c) Network time synchronization
(d) Network backup over LAN
(e) Task-to-task communications to external computers
(f) LAN global naming facilities.
(g) Remote procedure call
(h) Remote terminal session

4.4.4 Security Services

The security solution shall comprise of comprehensive solution for secured zone Firewalls i..e LAN Firewall & Gateway Firewall, intrusion Prevention system IPS (Network based & Host based) & Strong Authentication (multi layered), LDAP , Encryption mechanism. The contractor shall provide a tightly integrated intrusion detection system to detect and prevent intrusion

Followings are the functional requirement from the security system:

- System shall have Multilayer (at least network, application layer) firewall which shall protect the complete system network from unwanted users. Further the separate firewall of different OEMs shall be provided to take care the security of all the servers & shall have High Availability architecture with No Single Point of Failure (NSPOF).

- Gateway Firewall should be capable of load balancing multiple links from different service providers.

- LAN Firewall shall provide isolation/security services between the subsystems installed under SCADA system of R-APDRP

- Firewalls deployed should not become a bottleneck. It shall be Robust, Secure, Scalable and future-proof with Centralized Management.

- Two type of IPS Host based & Network based shall be deployed with minimum hardware & they should not go blind in peak traffics.

- IPS should have hybrid technology to detect attacks. It should detect through a combination of Protocol Anomaly and Signature matching.

- Shall have Gateway antivirus which will protect from inflow of virus from the Internet and other WAN locations at the gateway itself with content filtering without any lag in data transmission.

- Shall have strong authentication containing user name and passwords which shall be very difficult to compromise.

- SSL over VPN to provide secured link over public network such as with RTU/FRTU/FPI

4.4.4.1 Features

Followings are the features specific to each component of security system

4.4.4.1.1 Firewall

The Firewall shall be hardware box Firewall system with following features.

- Firewall speed >250 Mbps
- Data encryption supported DES (56 bits) 3 DES (168 bits) and hashing algorithm like MD5 and SHA-1
- Encryption to offload the main CPU
- It shall have minimum 8 Ethernet 10/100 /1000 ports (4ports for connectivity to two web servers & 4 Ports for connectivity to LAN
- Support NAT and PAT
- Capability of working in Load sharing and hot standby mode
- Denial of service prevention.
- DNS guard features
- JAVA and ActiveX blocking
- Radius integration
- Web based management interface
- Stateful inspection for web, mail, SQL application etc.
- Detailed system logging and accounting feature
- No. of concurrent TCP Sessions supported shall be more than 5000.

4.4.4.1.2 Intrusion Prevention System (IPS)

The contractor shall provide a tightly integrated intrusion detection & prevention system Capable for detecting the intrusion attempt that may take place and intrusion in progress and any that has taken place.

Both Network based and Host based IPS should have centralized Management Console system which will be either the application server with NMS or any of the workstation. The Centralized management console shall have integrated event database & reporting system & it must be able to create and deploy new policies, collect and archive audit log for post event analysis. The system shall have Integrated Event Database & Reporting System. Automated Update of the signature for two years shall be provided and there should be provision for creating customized signature

(A) **Intrusion Prevention System (Network Based)**

- After detecting any intrusion attempt there should be provision to configure to perform the following functions:
    - Capability for Detecting the intrusion attempt that may take place, intrusion in progress and the intrusion that has taken place
    - Reconfigure the firewall provided in this package.
    - Beep or play a .WAV file
    - Send an SNMP Trap datagram to the management console. The NMS server envisaged under the specification shall be used as management console also.
    - Send an event to the event log.
    - Send E-mail to an administrator to notify of the attack.
    - Save the attack information (Timestamp, intruder IP address, victim IP address/port, protocol information).
    - Save a trace file of the raw packets for later analysis
    - Launch a separate program to handle the event
    - Forge a TCP FIN packet to force a connection to terminate.
    - Detect multiple forms of illicit network activity: -Attempted
    - Vulnerability Exploits -Worms -Trojans -Network Scans -Malformed Traffic -Login Activity
    - The System shall support monitoring of multiple networks. The system shall also support the monitoring of additions or changes to addresses of devices on the network.

The system shall have detection rules for monitoring faults, dangerous and malicious activity related to IP based protocols. The Contractor shall also apply its power control and security experience to enhance these detection rules for specific issues within the system.

(B) **Intrusion Prevention System (Host Based)**

Host based IPS shall run on the servers. After detecting any intrusion attempt there shall be provision to configure the IPS to perform following actions

- Send an SNMP Trap datagram to the management console. The NMS server envisaged under the specification shall be used as management console also.
- Send an event to the event log. Send e-mail to an administrator to notify of the attack.
- It should be capable of creating audit trail for user and file access activity, including file accesses, changes to file permissions, attempts to install new executables and/or attempts to access privileged services,
- In an event where user accounts are added, deleted, or modified changes to key system files and executables is done in by unauthorized account or there is unauthorized attempt to overwrite vital system files, to install Trojan horses or backdoors, suitable action shall be taken such as :
    - Terminate user Login (intruder)
    - Disable user Account (intruder)
    - Administrator can define the action to be taken
    - Forge a TCP FIN Packet to force a intruder connection to terminate.
- Should provided events check for suspicious file transfers, denied login attempts, physical messages (like an Ethernet interface set to promiscuous mode) and system reboots.

4.4.4.1.3 Gateway Antivirus

This shall be used for Gateway scanning of viruses. Gateway antivirus shall have Centralized-user Administration which will Communicate directly with centralized user directories such as LDAP. It shall have the all the essential/standard features of Latest version of Gateway antivirus, some of the features are as following:

- It shall have Policy-based URL filtering and Dynamic Document Review.
- It shall protect web traffic with high-performance, integrated virus scanning and web content filtering at the gateway
- It shall ensure protection by combining list-based prevention with heuristic content analysis for both virus protection and web content filtering
- It shall eliminate unwanted content and malicious code & Scan all incoming and outgoing HTTP and FTP traffic etc.

The Security System shall use the best practices to prevent the System itself being a source of security compromise. The System shall be hardened, patched, tested, and designed with security as a primary objective. Communication with (GUI and notifications) and within (agent

reporting and updates) the System shall use encryption and authentication.

4.4.4.2 Other aspects of security

4.4.4.2.1 Application Security Monitoring

The standard operating system shall support the monitoring of security on host installed applications. The system shall support or allow the creation of monitoring for:

- Application Software Error Conditions
- Application Software Performance Issues
- Application Configuration Changes
- Application Logins, etc.

4.4.4.2.2 Security Alarms

The system shall be capable of annunciation, to include audible and visual alarms and remote paging whenever a security event takes place and shall support the following:

- Instant notification through email or pager
- Logical grouping of security events by time, location, and device, etc
- Interactive dashboard window for viewing and acknowledgement

4.4.4.2.3 Analysis and Reports

- The system with the stored information, shall be able to produce analyses and reports to meet security compliance requirements. The system shall be equipped with best practices ad-hoc reports widely used in the industry.
- The employer's personnel shall be trained to be capable of creating new custom analysis and reports, and revising existing, without requiring external consultation.

4.4.4.2.4 Log Archiving

The security system shall archive, record, and store all security related events in raw form for at least one year. As a minimum, the event logger shall record all security related events from the perimeter security devices and the host IPS. Graphical trend displays of each event shall be available along with specific information on the type of intrusion, the area affected and the source via IP address.

4.4.4.2.5 Data Access through intranet

The Web server at Control Center is to function as source of information on the distribution network. It will be accessed by utility intranet user. Any additional

client software, if required, at external clients/users ends, the same shall be made dynamically available from Web server for its downloading by these external clients. There shall not be any restriction to the number of clients downloading this software (i.e. Unlimited number of client downloads shall be provided).

The external users shall be licensed users of the employer.

The following features are required:

a) The Web servers shall be sized to support atleast 50 concurrent external intranet clients/users for providing access to real-time data.

b) External intranet clients/users shall be connected to the web servers through secure authentication such as VPN access. These users shall be denied direct access to the SCADA/DMS protected LAN.

c) Internal SCADA/DMS users shall not have any dependency on the availability of the Web servers.

d) For the purpose of transfer of data/displays/ from the SCADA/DMS system to the Web server system, the SCADA/DMS system shall initiate a session with the Web server and any attempt to initiate a session by the Web server shall be terminated by the Firewall in SCADA/DMS system LAN. Interface between Web server and SCADA/DMS zone shall preclude the possibility of external clients defining new data/Report/Displays.

   For any sessions initiating from the DMZ LAN into the protected LAN, the servers shall be located in a separate DMZ LAN that will be isolated from common applications connected directly to ISP such as email. The Access to these servers from the external web will be through authorization of Virtual Private Network.

e) The web server shall provide access to allowable real time data and displays, at defined periodicity, for viewing by external clients/users. The access to each display shall be definable on per user type basis. It shall be possible to define up to 100 users. Further the SCADA/DMS system administrator shall exercise control over the real-time displays which can be accessed through the Web server.

f) The Web server at Control Center shall also facilitate exchange of email messages from ISP (Internet Service Provider) and other mail servers supporting SMTP..

g) Suitable load balancing shall be provided among the web servers where each shall serve proportionate number of clients. However in case of failure of one of the servers, all the clients shall automatically switch to the other web server(s).

Typical displays/pages for Intranet access shall be same as that on the SCADA/DMS**.** Real time SCADA data on web server shall be refreshed every minute

The access to Web server/site shall be controlled through User ID and password to be maintained /granted by a system administrator. Further, different pages/data access shall be limited by user type (i.e. CMD,, Mgmt user, incharge etc). The access mechanism shall identify and allow configuration of priority access to selected users.

Further, tools shall be provided for maintaining the website, web server configuration, E-mail configuration, FTP configuration, Mailing lists setup and customer support. Latest protections against viruses shall be provided.

4.4.4.2.6 Signature Updating Requirements

The system shall be able to accept timely updates. The updates shall keep the threat signatures current, providing the latest detection and protection. The updates shall also incorporate the latest security enhancements into the Security Management System. These enhancements shall increase security and functionality, without requiring redesign or reengineering efforts.

4.4.4.2.7 Network Management system (NMS)

A network monitoring and administration tool shall be provided. The interface of this tool shall show the DMS hardware configuration in form of a map. The network-monitoring tool shall automatically discover the equipment to construct the map. It shall support management of multi Vendor network hardware, printers, servers and workstations.

It shall support remote administration of network devices, management of thresholds for monitoring performance and generation of alarm and event notifications. It shall be possible to send these notifications to maintenance personnel through e-mail

The Network management system shall manage the interfaces to the SCADA/DMS servers, workstations, devices, communication interface equipment, and all SCADA/DMS gateways and routers ,switches etc

The network management software shall be based on the Simple Network Management Protocol (SNMP-Internet RFC 1157) over TCP/IP (CMOT), with additional proxy software extensions as needed to manage SCADA/DMS resources.

The NMS software shall provide the following network management capabilities:

(a) Configuration management
(b) Fault management
(c) Performance monitoring.

The network management software shall:

(a) Maintain performance, resource usage, and error statistics for all of the above interfaces (i.e. servers, workstation consoles, devices, telephone

circuit interface equipment, and all SCADA/DMS gateways , routers etc) and present this information via displays, periodic reports, and on-demand reports.

The above information shall be collected and stored at user configurable periodicities i.e. upto 60 minutes. The Network Management System (NMS) shall be capable of storing the above data for a period of one year at periodicity of 5 minutes.

(b) Maintain a graphical display of network connectivity to the remote end routers

(c) Maintain a graphical display for connectivity and status of servers and peripheral devices for local area network.

(d) Issue alarms when error conditions or resource usage problems occur.

(e) Provide facilities to add and delete addresses and links, control data blocks, and set data transmission and reception parameters.

(f) Provide facilities for path and routing control and queue space control.

4.5 Database structure

The SCADA/DMS RTDB (Real Time Data Base) shall be an active process model. i.e. It shall initiate actions or events based on the input it receives. The RTDB shall describe the state of the power system at a given point in time and the events that move the system to a new state at the next point in time. This database is required to support the data access to real time information and to allow efficient integration and update.

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

The SCADA/DMS shall include a single logical repository for all data needed to model the historical, current, and future state of the power system and SCADA/DMS – the Source Database (SDB). All information needed to describe the models on which the SCADA/DMS operates, shall be defined once in the

SDB and made available to all SCADA/DMS applications, real-time database, and user interface maintenance tools that need the information.

Any database update, whether due to local changes or imported network model changes, shall be able to be placed online in a controlled manner without causing undue interruption to network operations, including without losing any manually entered data. For example, a network model update to introduce a new substation shall not interrupt the ability to perform supervisory control actions or receive telemetry to view the network state. It shall be possible the changes, local or imported, to be placed online either automatically or under manual control with proper validation. It shall be possible to easily revert to an earlier database version, again without undue interruption to network operations. The capability to import & export the CIM compliant network model data including the corresponding telemetry and ICCP data reference in XML format to send it to other parties shall be provided. The capability to import the CIM compliant network model data from other parties in XML format shall also be provided.

The SCADA/DMS shall provide a consistent interface to accept XML format data for updates from other database applications; and provide a consistent interface to import & export data in XML format.

4.5.1 Software Maintenance and Development Tools

4.5.1.1 General requirements

A set of software shall be provided to enable maintenance of application software and development of new software in software development mode.

All hardware and software facilities shall be provided to allow creation, modification and debugging of programs in all languages that are supplied.

The following shall thus be possible:

- Program and data editing
- Program compiling and assembling
- Linking
- Loading, executing and debugging program.
- Version management
- Concurrent development

The following features shall be provided:

- Library management
- Programs allowing to copy and print any data or program files
- Backup and restore
- File comparison

- Sort and merge
- Programs that allow to partially save and recover volumes
- Core and memory dump.

In addition tools shall have the following:

4.5.1.2 Command language

A complete command language shall be provided that allows interactive use of any console to interactively create, modify and debug programs in all languages provided. It should also be possible to create and save command procedure file and to execute it sequentially.

4.5.1.3Linkage Editor and Loader

Compilers and assemblers, linkage editor and loader shall be provided to link object modules from an assembly or compilation to produce an executable module and load it in system. As far as possible, the loader shall accept object modules issued from various language compilers.

4.5.1.4 Symbolic Debugger

A language-independent, interactive symbolic debugger shall be provided to enable the user to test new software and inspect the characteristics of existing software. The execution of a program shall be under the control of the debugger according to parameters entered by the user. The following features shall be supported:

(a) Program execution breakpoint control
(b) Program execution sequence tracing
(c) Display and modification of program variables
(d) Attachment of specifically written debug code to the program under test.

The debugger shall allow halting execution of a program at predefined points, reading and modifying the registers and memory locations and executing step by step a program. Tender shall describe the features of debuggers for each type of equipment.

4.5.1.5 System Integration

System integration services shall be provided for adding new programs to the set of active software after the programs have been tested. These services shall include commands to substitute one program for another, to set up or modify operating system tables, and to schedule and activate a new program with a minimum of interference with the normal running of the SCADA/DMS functions. The capability to restore the system to its status prior to the new program integration shall be provided.

4.5.1.6 System Generation

System generation software and procedures shall be provided to generate an executable object code of all software, databases, displays,

and reports. Employer personnel shall be able to perform a system generation on site, using only equipment, software, procedures, and documentation supplied with the SCADA/DMS. It shall not be necessary to return to the Contractor's facility or rely on the assistance of Contractor personnel.

The procedures necessary to perform a complete system generation shall be provided as interactive or batch commands maintained on auxiliary memory and on archive storage, source listings, and detailed manuals. System generation shall be accomplished without programming; only directives or control commands described in the procedures shall be required.

4.5.1.7 Code Management

A code management utility shall be provided for documenting and controlling revisions to all SCADA/DMS application programs. The utility shall maintain a library of source, object, and executable image code and provide a controlled means for changing library files containing this code.

The code management utility shall include inventory, version, and change control and reporting features. Program dependencies shall be included in the library for user reference. The code management facility shall retain a complete history of additions, deletions, and modifications of library files.

An integrated source code development subsystem supporting C, Fortran, Java, and C++, other programming languages used in the SCADA/DMS shall provide a software configuration management system to define the elements and the associated attributes of the applications provided in the SCADA/DMS. Source definitions for all elements of an application shall be maintained in disk files under a code management system. As a minimum, the code management system shall:

1) Manage source code and binary images

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

3) Manage documentation modules and associate them with source 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

4.6 Database Development software

The databases organization shall be designed to meet the following major functional requirements:

- Data consistency,
- Compliance with the system performance requirements including both response times
- and expansion capabilities,

A Database development software shall be provided which shall contain database structure definitions and all initialisation data to support the generation of all relational , real time database (RTDB)non-relational run-time databases required to implement the functions of SCADA/DMS system. All the facilities required for generating, integrating and testing of the database shall be provided with the SCADA/DMS system. The delivered SCADA/DMS database shall be sized for the ultimate system as described in this Specification. The database development facility shall be available on development system comprising of server & workstation. Once the database creation/ modification activity is over, the compiled runtime executables shall be downloaded to all respective machines. Executing the database generating functions shall not interfere with the on-line SCADA/DMS functions.

The database development function shall locate, order, retrieve, update, insert, and delete data; ensure database integrity; and provide for backup and recovery of database files. The database development function shall generate and modify all SCADA/DMS data by interfacing with all database structures. The location of database items shall be transparent to the user performing database maintenance.

Extensive reasonability, integrity, and referential integrity checks shall be made on user entries to detect errors at the time of entry. Invalid entries, such as entering an invalid data type or attempting to define contradictory characteristics for a database item, shall be detected and reported to the user in an error message. All error messages shall be in plain English. The user shall not be required to repeat steps that were correctly executed prior to the erroneous action. Help displays shall be available to provide additional, detailed information to the user on request.

All newly defined points shall be initially presented to the user with default values for all parameters and characteristics where defaults are meaningful. It shall also be possible to initialise a new database point description to an existing database point description. The user shall be guided to enter new data, confirm existing data, and change default values as desired.

All required entries for any database item selected for changes shall be presented to the user. When parameters are entered that require other parameters to be specified, the additional queries, prompts, and display areas required to define the additional parameters shall be presented automatically.

(a) Add, modify, and delete telemetered, non-telemetered, or calculated database items and data sources such as RTUs/ FRTUs / FPI, data links, and local I/O.
(b) Add, modify, and delete application program data
(c) Create a new database attribute or new database type
(d) Resize the entire database or a subset of the database
(e) Redefine the structure of any portion of the database.

The database tool for creation, editing, generation, export, import of ICCP database including complete definition, association, bilateral tables, objects etc shall be provided.

4.6.1 Run-Time Database Generation and Maintenance

The database development software shall generate incremental database changes as well as run-time (loadable) databases from the global source database (user entered database) Incremental structure changes in the source database such as addition of a bay or a substation shall not require regeneration of the entire run-time database. Based on the nature of the change, the database development software shall determine which portion of the database must be regenerated and which displays, reports, and software functions must be re-linked.

All errors that were not detected during data entry time but are encountered during run-time database generation shall be flagged. The database generation routines shall continue processing the database in an effort to detect all errors present in the database before terminating the generation task.

4.6.1.1 Data Retention

The database generation process shall retain and utilize data from the current SCADA/DMS database in the newly generated database, even when a newly generated database contains structure changes. Data to be retained across database generation cycles shall include, but not be limited to, quality codes, manual entries, tags, historical data, and tuning parameters.

4.6.1.2 Making Database Online

After an error-free database generation, the user shall be able to test the data-base in an off-line server prior to its use in an on-line server. The previous run-time database of the server shall be archived such that it is available to replace the new database upon demand. The archived database shall be deleted only when directed by the user.

Newly generated run-time databases shall only be placed on-line by user command. Following the assignment of a new database to a server and on user demand, the database management software shall access each SCADA/DMS

server to ensure that all databases are consistent. Inconsistencies shall be annunciated to the user.

4.6.1.3 On-Line Database Editing

Selected database management functions and changes to a run-time database shall be possible without requiring a database generation. These shall be limited to viewing functions and changes to the contents, but not the structure of the database. On-line changes shall be implemented in all applicable SCADA/DMS run-time databases without system downtime. Changes shall also be implemented in the global database to ensure that the changes are not lost if a database regeneration is performed. On-line database editing shall not affect the SCADA/DMS system's reaction to hardware and software failures nor shall it require suspension of exchange of data among servers for backup purposes.

4.6.1.4 Tracking Database Changes

The database manager utility shall maintain Audit trail files for all changes made by all users. The audit trails shall identify each change including date and time stamp for each change, and identify the user making the change. An audit trail of atleast last 2 months shall be maintained and another audit trail maintaining records of who/when performed the edit operation shall be maintained for a period atleast 2 months.

4.6.1.5 Initial Database Generation

The initial database shall contain all data required by the SCADA/DMS systems. Default values shall be used in consultation with the employer for data that is not provided by employer. Population and maintenance of the distribution network model should be possible by using the database maintenance tools to build the database from scratch. In addition if required data already exists within the Employer's corporate Geographic Information System (GIS) as a part of R-APDRP scheme or otherwise, the SCADA/DMS database functions should leverage this effort by providing an interface/adaptor to extract GIS data using the CIM international standard IEC 61970/61968 and automatically generate the complete Network Operations Model. The data extracted should include network device information, connectivity, topology, nominal status and non-electrical data such as cable ducts , landbase data etc . Further Land base data can be sourced from GIS in Shape files or DXF.

4.7 Display Generation and Management

SCADA/DMS displays shall be generated and edited using interactive display generation software delivered with the system. The display generator shall be

available on development system & once the display/ displays creation/ modification activity is complete, the compiled runtime executables shall be downloaded on all workstations/servers.

The display editor shall support the important construction options like:

- Copy/move/delete/modify,
- Building at different zoom level,
- Linking of any defined graphics symbol to any database point,
- Pop-up menus,
- Protection of any data field on any display against user entry based on log-on
- identifiers
- Activation of new or modified displays for any application or across all applications of the system by a simple command that causes no noticeable interruption of on-line DMS system activity.

All displays, symbols, segments, and user interaction fields shall be maintained in libraries. The size of any library and the number of libraries shall not be constrained by software. The display generator shall support the creation, editing, and deletion of libraries, including copying of elements within a library and copying of similar elements across libraries. A standard set of libraries and libraries of all display elements used in the delivered SCADA/DMS system shall be provided.

Displays shall be generated in an interactive mode. The user shall be able to interactively:

(a) Develop display elements
(b) Link display elements to the database via symbolic point names
(c) Establish display element dynamics via database linkages
(d) Define linkages to other displays and programs
(e) Combine elements and linkages into display layers
(f) Combine display layers into displays.

The display generation, compilation & loading shall not interfere with the on line SCADA/DMS functions.

All user interface features defined in this Specification shall be supported by the display generator.

4.7.1 Display Elements

The elements available to create a display shall consist of graphic primitives symbols, segments, User Interaction Field and layers. These elements shall be

available to be linked to the SCADA/DMS functions and dynamically transformed on the display as governed by linkages to the database.

4.7.1.1 Segments

The display generator shall support the construction of display segments consisting of symbols, primitives, and dynamic linkages to the database and user interface. Typical uses of display segments are pull-down menus, bar charts, and common circuit breaker representations. The display generator shall be able to save display segments in segment libraries for later use. The SCADA/DMS system shall include a base library of segments commonly used by display builders.

The display generator shall support the addition, deletion, and modification of segments, including the merging of one segment with another to create a new segment. Segment size shall not be limited. Segments shall be defined at an arbitrary scale factor selected by the user.

4.7.1.2 Dynamic Transformation Linkages

Dynamic transformations shall be performed on symbols and display segments based upon dynamic linkages to database variables. All linkages to the database shall be defined via symbolic point names. Each symbol or segment stored in a library shall include its dynamic transformation linkages, although the specific point names shall be excluded. Dynamic transformation linkages shall support the dynamic data presentation.

4.7.2 Display Generation and Integration

The displays shall be constructed from the display elements described above. The display definition shall allow displays to be sized to meet the requirements of the SCADA/DMS application for which they are used; displays shall not be limited by the size of the viewable area of the screen. The display generation software shall allow unbroken viewing of the display image being built as the user extends the size of the display beyond the screen size limits. Each display shall include the display coordinates definition that will permit a user to navigate successfully to the portion of the display that is of interest.

It shall be possible for a user to build a new display starting with a blank screen or an existing display. The definition of each layer shall include a range of scale factors over which the layer shall be visible. The display generator shall also support manual control of layer visibility, where the user of the display shall determine the layers on view. Each display may incorporate manually and automatically (by scale factor) displayed layers. The user shall also define the periodic update rate of the dynamic information on the display and any programs called before or after presentation of the display.

The display generator shall support the integration of new and edited displays into the active display library. During an edit session, the display generation software shall allow the user to store and recall any display. To protect against loss of display work when computer fails, the current work shall be automatically saved every 5 minutes (user adjustable) to an auxiliary memory file.

The display generator shall verify that the display is complete and error-free before integrating the display into the active display library. A copy of previous display library shall be saved & protected and it shall be brought back on line or can be deleted upon user request.. It shall not be necessary to regenerate any display following a complete or partial system or database generation unless the database points linked to the display have been modified or deleted.

4.7.2.1 Imported CADD Drawings

The display generator shall support the import of drawings, including power system one-line diagrams, developed by owner on Computer Aided Drafting and Design (CADD) systems. The drawings may be used in the SCADA/DMS system as the static background for displays. The display generator shall provide the capability to add, delete, and modify the dynamic information supplied to the drawings using the specified features of the display generation and management software. As necessary, employer will replace the static background by importing a new drawing from the CADD system and re-linking associated database elements. The display generator shall allow a user to update the dynamic information to reflect any changes required by the updated drawing.

4.8 Report Generation Software

The SCADA/DMS system shall include report generation software to generate new report formats for SCADA/DMS and edit existing report formats. The user shall be guided in defining the basic parameters of the report, such as the report database linkages as symbolic point names, the report format, the report activation criteria, the report destination (workstation, printer, or text file), and the retention period for the report data.

The user shall be able to construct periodic reports and ad-hoc queries via interactive procedures. The capability to format reports for workstations and printers shall be provided. The user shall be able to specify the presentation format for periodic reports and ad-hoc query reports as alphanumeric display format, graphical display format, or alphanumeric printer format. The user shall be able to specify that processing functions, such as summations and other arithmetic functions, be applied to portions of the report data when the report is processed for display, printing, or file storage. The software shall provide for generation of reports that are the full character width of the printers and that use all of the printer's capabilities, such as font sizes and styles and print orientation.

For report data editing, the user shall be able to obtain the data from a retained report, modify the data, repeat the inherent data calculations, reprint the report,

and save it in a report retention file on auxiliary memory without destroying the original report.

The user shall also be able to access a retained report, modify its point linkages to the database, modify its format, and save it in a report retention file on auxiliary memory as a new report without destroying the original report.

Executing the report generating functions shall not interfere in any server of the system with the on-line SCADA/DMS functions.

4.9 System Generation and Build

System generation includes the activity of generating an executable object code of all databases, displays, and reports as required for SCADA/DMS system. System build is the process under which all the above executables and the executables provided for SCADA/DMS application software are ported to the SCADA/DMS system hardware and configuring to make it operational.

The contractor shall do the complete system generation and build as required for successful operation of the SCADA/DMS system. The contractor shall also provide the complete backup of the SCADA/DMS system in electronic media such as tapes, CDs, MO disks etc. Employer personnel shall be able to restore the SCADA/DMS system at site by using above backup tapes/CDs etc. The contractor shall provide the procedures necessary to restore the system from the backup tapes/CDs etc. The DR system shall always have updated set of system build . It shall be synchronised with the SCADA/DMS control centre .

4.10 Software Utilities

All software utilities used to maintain SCADA/DMS software, whether or not specifically required by this Specification, shall be delivered with the system.

The software utilities shall operate on-line (in background mode) without jeopardizing other SCADA/DMS application functions that are running concurrently. This utility software shall be accessible from workstations, programming terminals, and command files on auxiliary memory. Multiple users shall have concurrent access to a utility program task, provided there are no conflicts in the use of peripheral devices.

4.10.1 File Management Utility

File management utilities shall be provided that allocate, create, modify, copy, search, list, compress, expand, sort, merge, and delete program files, display files, and data files on auxiliary memory and archive storage.

4.10.2 Auxiliary Memory Backup Utility

A utility to backup auxiliary memory of server and workstation files onto a user-selected auxiliary memory or archive device shall be supplied. The backup utility shall allow for user selection of the files to be saved based on:

(a) Server and workstation
(b) File names (including directory and wildcard designations)
(c) File creation or modification date and time
(d) Whether or not the file was modified since the last backup.

A backup utility that can backup all server and workstation auxiliary memories on to a single target auxiliary memory or archive device shall be provided. The backup utility must ensure that the source auxiliary memory files are captured properly regardless of caching activity.

4.10.3 Failure Analysis Utility

Failure analysis Utility shall be provided to produce operating system and application program status data for analysing the cause of a fatal program failure. The failure information shall be presented in a condensed, user-oriented format to help the user find the source of the failure. The information shall be presented on displays and recorded for historical records and user-requested printed reports.

4.10.4 Diagnostic Utility

The system shall have suitable auto diagnostic feature, on line & offline diagnostic Utility for on-line and off-line monitoring for equipments of SCADA/DMS system shall be provided.

4.10.5 System utilisation Monitoring Utility

Software utility shall be provided in each server and workstation to monitor hardware and software resource utilisation continuously and gather statistics. The monitoring shall occur in real-time with a minimum of interference to the normal SCADA/DMS functions. The period over which the statistics are gathered shall be adjustable by the user, and the accumulated statistics shall be reset at the start of each period. The statistics shall be available for printout and display after each period and on demand during the period.

4.10.6 Other Utility Services

On line access to user and system manuals for all software/Hardware products (e.g., Operating System and Relational Database Software/hardware) and SCADA/DMS applications shall be provided with computer system.

End of Section 2, Chapter 4