Technical Specifications for Implementation of Unified Load Despatch and Communication (ULDC) Phase-III "SCADA/EMS Upgradation Project-Eastern Region SLDCs and RLDC"

POWER GRID CORPORATION OF INDIA LIMITED

Volume-II

Technical Specification

for Implementation of

Unified Load Despatch and Communication

(ULDC) Phase-III

"SCADA/EMS upgradation Project

Eastern Region SLDCs and RLDC"

VOLUME-II

(PART-A, B,C,D,E)

CONTENTS

P A R T – A

SECTIONS

APPENDICES

PART – B

SECTIONS

APPENDICES

P A R T – C

SECTIONS

APPENDICES

P A R T – D

SECTIONS

APPENDICES

P A R T – E

SECTIONS

Section 1

General Requirements of the Project

Table of Contents

Section1 Introduction and General Information

1.1 Introduction

The intent of this specification is to replace/upgrade the Supervisory Control and Data Acquisition System and Energy Management System (SCADA/EMS) of Eastern region Regional Load Dispatch Centre (RLDCs) and State Load Dispatch Centers (SLDCs). This Volume II (Part A to Part E) of the Tender Document describes the technical specification for the following systems:

Part-A : General Information of the Project

Part-B : Technical specification of SCADA/EMS System

Part-C : Auxiliary Power Supply & DG Set

Part-D : Remote Terminal Unit (RTU)

Part-E : Video Conferencing System

The purpose of this Section-1 of Part A of the technical specification is to provide scope of work, overview of the Project, general information about the existing systems and the proposed system under this project, requirements, responsibilities & obligations of contractor, Employer & Owner and general bidding requirements for the project.

1.2 Indian Power Sector

The Power Sector in India is organized in five electrical regions for operation of power system namely North, South, East, West and North-east. All the regions are synchronized as single grid.

The exchange of power takes place through 765/400/220KV transmission lines and HVDC interconnections. The operation of each regional grid is managed by the Regional Load Dispatch Centre (RLDC) with underlying State Load Dispatch Centre (SLDCs). At the National level, to supervise the RLDCs and to monitor the interregional power exchanges, a National Load Dispatch Centre at New Delhi is in operation. All SLDCs, RLDCs and NLDC control Centers are equipped with SCADA/EMS systems and WAMS systems and Renewable Energy Management System (REMC).

1.3 Owner

States/Union Territories shall be the "**Owner**" of the respective State Load Dispatch Centre's and GRID-INDIA/RLDC shall be the "**Owner**" for RLDC portion of work.

1.4 POWERGRID

POWERGRID, a Govt. of India Enterprise, "a schedule 'A', 'Maharatna' Company" and is one of the Largest Transmission Utility in the World and is playing a strategic role in the development of Indian Power Sector . POWERGRID is responsible for establishment and operation of inter-state EHV transmission lines, substations and communication facilities in a coordinated and efficient manner. This gigantic transmission network, spread over length and breadth of the country, is consistently maintained at an availability of over 99% through deployment of state-of-the-art Operation & Maintenance techniques which are at par with Global Standards. About 51% of total power generated in the country is wheeled through POWERGRID's transmission network.

POWERGRID shall be the "**Employer**" for all SLDCs and GRID-INDIA, ERLDC shall be the "**Employer**" for ERLDC.

POWERGRID shall be "**Consultant**" for ERLDC (GRID-INDIA) for this project.

1.5 Eastern region constituents:

The Eastern Region Power System Interconnects the Generation, Transmission and Distribution facilities of State utilities. The scope of this project includes implementation of SCADA/EMS system for following constituents:

- GRID-INDIA Eastern Regional Load Despatch Centre
- Damodar Valley Corporation (DVC)
- West Bengal State Electricity Transmission Company Limited (WBSETCL)
- Orissa Power Transmission Corporation Limited (OPTCL)
- Jharkhand Urja Snacharan Nigam Limited (JUSNL)
- Bihar State Power Transmission Power Corporation limited (BSPTCL)
- Energy & Power department, Govt. of Sikkim (SIKKIM)

Note: Details of New Control Centres being established under this Project is as per Part-A, Appendix-H.

1.6 Present Load Despatch and Communication Facilities in Various Region

Load dispatch & Communication facilities presently available in Various Region RLDC/SLDCs were commissioned in 2016-2017 under SCADA Replacement/Upgradation Project. Load dispatch & Communication facilities has been established in the hierarchical order which includes Regional Load Despatch Centre (RLDC) at the apex level and the Remote Terminal Units (RTUs)/SAS at Power Station/Sub-station at the lowest level as shown in Figure 1.1. In between there are State Load Despatch Centers (SLDC). The RTUs acquire and forward parameters like voltage, frequency,MW, MVAR, Breaker and Isolator Positions etc. to SLDC/RLDC in real time as per their jurisdiction/ownership.

The Central Sector data is directly transmitted to RLDC, and the state sector data is transmitted to SLDC/ALDC/Sub-LDCs in the respective state. For data exchange between Control Centers, ICCP protocol has been used. All the RTUs commissioned are communicating on IEC-60870-5-101/104 protocol. RLDC system has been integrated with NLDCs. Under ULDC (Unified Load Despatch & Communication) project, SCADA/EMS systems were established in the Region and States. These systems are being maintained by the respective SCADA OEM. Eastern Region Load Despatch and communication facilities is shown in figure 1.2.

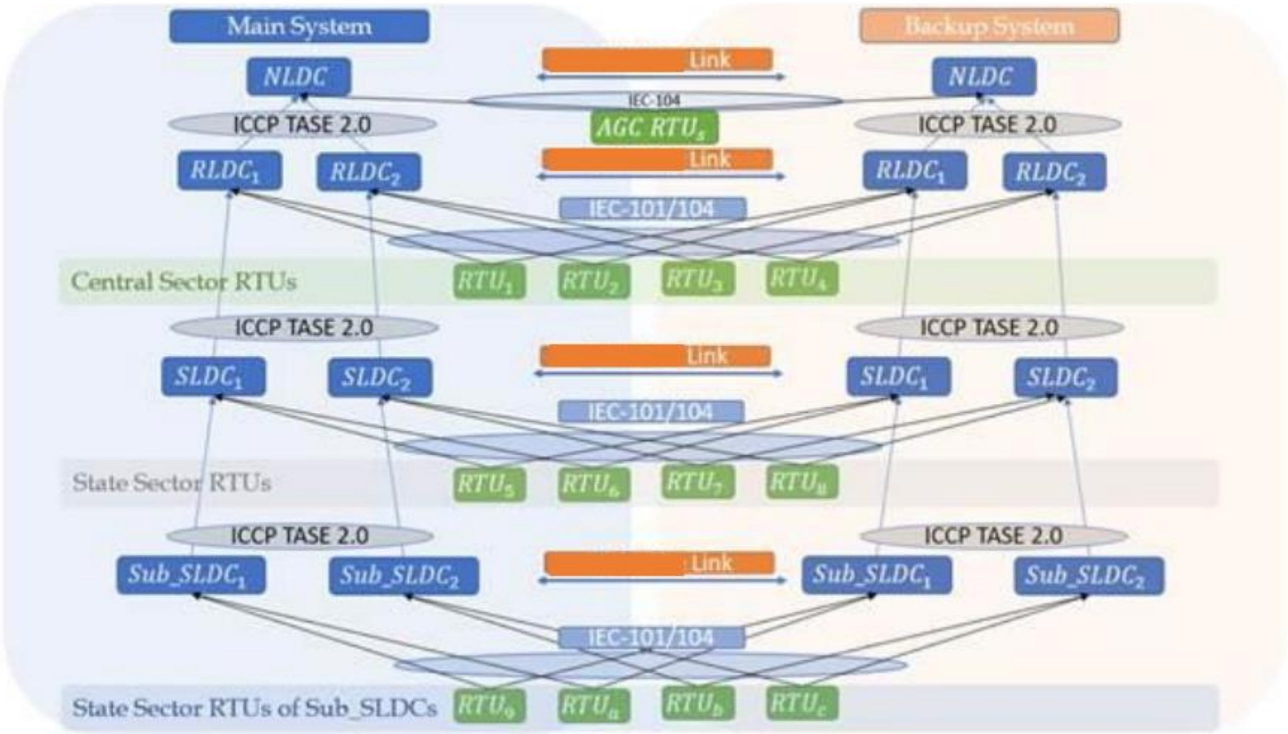


Figure 1.1: Existing Load Dispatch & Communication Facilities

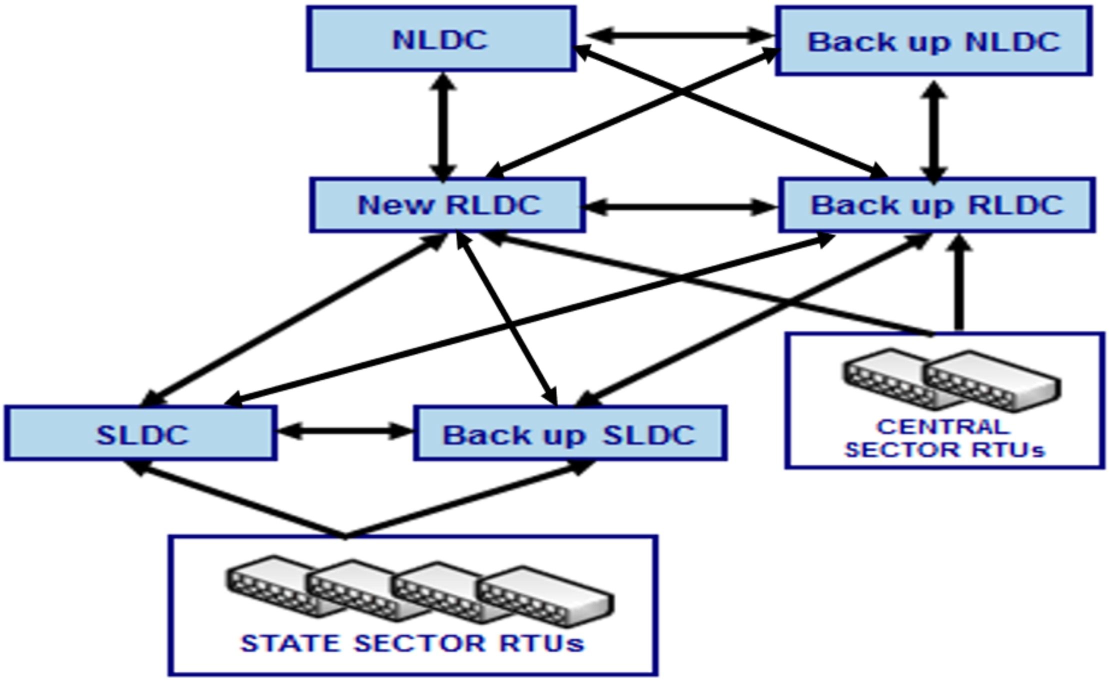


Figure 1.2: ER Load Dispatch & Communication Facilities

1.7 Existing SCADA/EMS systems at Load Dispatch Centers (LDCs) of various regions

The existing SCADA/EMS system includes the following subsystems:

- SCADA/EMS servers- To Support the functions of SCADA, Real-time Dispatching, Power System Analysis functions.
- Communication Front-Ends (CFEs) that drives the serial communication lines connected to the RTUs.
- ICCP (Inter-Control Centers Communications Protocol) servers that support inter-site data exchanges between Control Centers (Part-A Appendix-C).
- Historian server for Information Storage and Retrieval functions & is used for retrieval of stored data and Creation of Reports.
- DTS (Dispatcher Training Simulator) server and its associated DTS operator consoles that provide the dispatcher training capability. This is being used for the training purpose.
- Development Server is used to develop and maintain the SCADA/EMS software, displays and databases.
- Operator consoles and Video Projection System that handle the man-machine interface for system control and supervision operations.
- Network Management Console that provides the Configuration management, fault management and performance monitoring capabilities.

- WAN routers, in a redundant configuration, those allow several connections between Control Centers and with the Remote VDU (Video Display Unit).

- Peripheral equipment such as printers, satellite time receiver system (GPS).

- Data concentrator and protocol converters (DCPC)/Terminal server are installed at various locations to integrate the RTUs which are reporting over IEC 60870-5-101 Protocol.

1.8 Intent of the Project

This Volume II (Part A to E) of the Tender Document describes the project overview and the technical specifications for SCADA/EMS System to be procuredas a part of Implementation of this Project. The intent of this Project is:

- Installation of SCADA/EMS system at Main & Backup Control Centers of RLDC & SLDC. In this specification, Main Control centers shall be treated as Main 1 and Back up Control Centers shall be treated as Main 2 and both shall operate in ACTIVE-ACTIVE mode.

- Dismantling of existing/old SCADA/EMS system consisting of Hardware & Software at Main & Backup Control Centers of RLDC & SLDC.

- Integration of existing & new RTUs/Terminal server/DCPC/SAS with Main & Backup Control Centers, Terminal Server/DCPC installed at remote locations. List of locations where Terminal Server/DCPC are installed are in **Part-A, Appendix-H.**

- Installation of Terminal server and integration of it with existing RTU (**Part A Appendix B**)

- Integration of existing RTUs and Control Centers with new system shall not require any modification in the existing system.

- Change of setting by user or Auto adjustments specified in the specificationshall not require or result in any short of downtime/ unavailability of that system to the users.

- Integration of SCADA/EMS systems of other states SCADA system (which are not A to E of this project) with Main & backup control centers of RLDC & SLDC, which are part of the project.

- Integration with Offline Applications with Main and Backup SLDC.

- Integration of Wide area measurement system (WAMS-URTDSM)/Phasor Data concentrator (PDC) with Main and Backup Control Centers.

- Integration of Renewable Energy Control Centers with Main and Backup Control Centers.

- Developing & building new database from scratch for the project.

- Importing historical data from existing system to the proposed (new) system.

- In case of discrepancies observed in various sections of Technical Specification for the same requirement higher configuration /value shall be considered.

- Contractor shall provide presentation/demonstration of critical functions during technical evaluation of bid if requested by Employer.

The specification describes the functional and performance requirements of various components of the systems and sub-systems and maintenance & support services required from the Contractor under the aforesaid project. The delivered system should be robust enough to run all the critical functions without any interruption when one machine fails e.g., failure of one SCADA server or failure of a power supply in the **redundant** server should not interrupt the availability of the functions catered by the server.

System Network should be resilient enough to withstand single fault on network devices. It should be able to monitor multivendor network elements (Server, workstation, Router, switch, VPS cubes etc.). The Diagnostic software's shall be provided with the system to perform health monitoring of different components so that timely action can be taken e.g., VPS module health (e.g. CPU **RAM utilization etc**.) monitoring. Server CPU & **RAM** utilization can be monitored so that, before it goes beyond a percentage and system performance deteriorate, action can be taken. System should be secure against the cyber threats.

The measures should be taken to harden the system and make multiple level of defense e.g., firewalls supplied should be from different OEM in a Control Centre **as specified in Part-B section-5.** System should be flexible enough and it should be possible to do user interface related adjustment on-line without limiting operator options e.g., on-lining of new displays, adjustment of colour and brightness of VPS etc. shall not require downtime or image loss at any time to the operator. The entire performance requirements shall be demonstrated for the worst case, if requirements are not explicitly mentioned.

All the requirements of the specification are to be met by the delivered system. If there is any conflicting requirement, the applicable requirement shall be decided by the employer and that shall be binding on the Supplier. Backup Control Centre should be considered as independent CC (i.e., users are sitting at Backup CC and operating all the functions delivered even when Main CC is available) for licenses i.e., licenses for Backup CC should not be dependent on Main CC in anyway.

The purpose of this section (Part A) of the specification is to provide overview of the Project, general information about the existing systems, the proposed system under this project, requirements, responsibilities of Contractor as well as Employer/ Owner, general bidding requirements and the scope of work.

1.9 Overview of the Proposed Systems

Under this project new SCADA/EMS system shall be established at RLDC and SLDCs as per the intent given. The new system shall replace the existing system without affecting the operation of the existing system. The existing and new system shall be operated in parallel for minimum **three months** before shifting the entire operation to the new system. The bidder shall submit the migration philosophy document for each of the Constituent from the existing system to the new system along with the bid.

This document should include the details of the minimum space and logistics requirementat each of the existing control Centers, parallel operation with the existing system expected downtime in existing system, dismantling of the existing system and shiftingthe operation to the new system. The Back up Control Center should be able to perform all the functions of the Main Control Center except DTS. The system shall be designed for meeting identified expansion requirements in all respects including all hardware, software and configurations and the successful bidder shall have to demonstrate the same during Factory Acceptance Test. The overall scope of this project includes the Planning, Design, Engineering, Procurement and Implementation of SCADA/EMS Systems at Main & Backup Control Centers.

1.10 Scope of Work

The scope of work under this package shall include in complete conformity with all the sections of this Specification. This includes overall Project Management having Survey,Planning, Design, Engineering, Documentation, Integration, Supply, Delivery to site, Unloading, Insurance, Storing, Handling, transportation to final locations, Installation,Termination, Testing, Demonstration for acceptance, and Commissioning of following:

a) Supply and installation of Main & Backup SCADA/EMS computer system hardware and software along with associated items at respective Control Centers as per Appendix-G of Part-B, Vol-II. The new system shall be deployed in such a way that the operation of the existing systems (Main and Backup Control centers of RLDC and SLDCs) should not be disturbed. Both main and backup control center shall work in active-active mode and in case of failure of main control center backup shall come in role of main without any manual interruption (except commands/signals)

b) Integration of existing and New RTUs, SASs, DCPC/ Terminal server with Main and Back up Control Center System. The interoperability profile of existing RTUs is attached at Part-A, Appendix-B of this Section and for the remaining shall be provided during Engineering Stage. Each RTU shall report to Main and Back up Control Centers and suitable splitting (compatible with IEC 101/104) shall be used for redundancy at Front Ends of respective Control Centers. The devices required for integration of RTUs shall be in the scope of the contractor. The integration of existing and new RTUs at Control center end shall also be in the scope of the Contractor. Further, future bay integration shall not be treated as new RTU integration during AMC period, and any Bay extension during AMC shall be in the scope of the contractor without any commercial implication to the Owner. **The term AMC in this Specification shall be read as AMC including extension if any.**

c) Integration of Main and Back up Control Centers with **other** Control Centers on Mix mode ICCP protocol (i.e., new control centers are exchanging data on secure

ICCP and existing on plain ICCP and/or Secure ICCP protocol). Supplied system shall support simultaneous multiple bit encryption for SSL certificates for secure ICCP connection.

d) Integration of Main and back up control centers of SLDC with existing/new main and backup control centers of RLDCs (Regional Load Dispatch Center).

e) Integration of Main and back up control centers of RLDC with existing Control Centers such as main and backup control centers of NLDCs (National Load Dispatch Center), main and back up control centers of SLDCs of the region.

f) Integration of Main and Back up Control Centers on ICCP protocol with Distribution Companies.

g) A database development tool shall be provided at each Control Centre which shall import the data model from other control centers, validate the same at its own end and shall create ICCP database, historian database and SCADA/EMS database at each Control Centre including updation of ICCP bilateral table for fulfilling these requirements. The tool shall be independently operable and upgradable at each of the Control Centre.

h) Data exchange with URTDSM & Renewable Energy Control centers either on ICCP or IEC 60870-5-101/104 Protocol as per site/system requirement.

i) Collection & merging of SOE data at SLDCs & collection of SOE data from SLDCs, RTUs and merging at RLDC and transfer to Historian System at all Control Centers. Merging of SOE data required only if SOE is being transferred through file by RTUs. In case of SOE through ICCP, it shall be available in real-time. From historian and reporting system, all SOE shall be available.

j) All necessary protocol emulations required to integrate the existing RTUs, SASs andexisting Control Centers without affecting the data at the existing Control Center.

k) Development of complete Database, displays and reports either from scratch or by extracting existing database, displays and reports. The text available in displays and reports shall have support of fonts for English and Hindi and local etc. Contractor shall develop and provide tools to convert CIM files for different versions based on customized CIM-profiles in the files used by vendors system. The displays shall comply with the Display Building guidelines as per Appendix of vol-II.

l) Data Exchange with test bench DDS (Database Development System) on ICCP by new control center and on IEC 60870-5- 104/101 protocol by new RTUs for testing before integrating with real time system.

m) All type of data exchange to/from the different applications of the complete system shall be in secure manner ensuring latest cyber security guidelines from statutory authorities (CEA, NCIIPC, CERT-In etc.) throughout the period of contract, considering all the amendments issued from time-to-time.

n) Integration and operation of existing equipment's/devices, if any, to be utilized during contract period as mentioned in TS.

o) Import and Adaption of database & displays made by Owner for existing SCADA/EMS system including import historical data stored in existing Historical servers in new Historian System. Scope also includes the development of the required software tool to acquire the database/displays from the existing system, if required by contractor to perform this activity. All the features envisaged for the historian shall also be applicable for imported data from other systems.

p) Supply, Installation and Commissioning of RTU and Terminal server/DCPC wherever applicable.

q) Supply, Installation and Commissioning of Auxiliary Power System Comprising of UPS with Battery set, and DG set along with all necessary distribution board wherever applicable.

r) Supply of Spares identified under AMC along with main items to meet the contingency during installation period and during AMC period

s) All cabling, wiring, dressing, tagging, ferruling and interconnections to the equipment being supplied and to be integrated including communication equipment and power supply. All the supplied cables under the project shall be shielded type. Any cabling required for integration/interconnection of the supplied system with the existing equipment's shall also be in the scope of the Contractor.

t) Integration of all the supplied equipment and existing system.

u) The contractor's scope shall include customization of its ICCP protocol, such as configuration of ICCP database for ICCP name, scan period and all other – database parameters required to integrate existing Control Centers successfully.

v) The contractor's scope shall include customization of its IEC-60870-5-101 & 60870-5-104 protocols, such as configuration of database, scan period and all other database parameters required to integrate existing RTUs and SAS successfully.

w) Dismantling, Shifting of existing system and installation of new system at temporary location in parallel for intervening period.

x) Shifting and Installation of new system including server racks and panels after renovation of Control Center. This shall include all the services including cabling, interface modification and shifting or re-shifting of system required for intervening period and for final shifting to main Control Center. Re-cabling for some or all equipment as required for final shifting shall also be in the scope of supplier. All LAN cabling /power cabling etc. required for this activity shall be under the scope of supplier.

y) Dismantling of existing system (RLDC/ SLDC) after successful shifting of Operation to New Control Center. The existing system after dismantling shall be taken away by the contractor. The new system and existing system **shall run in parallel for at least Three months** before the dismantling of existing system. The contractor shall quote the buyback price for the dismantled system and this factor shall be taken into consideration while quoting the price bid. This shall include all the services including cabling and interface modification required for intervening period before final shifting to main Control center. **The provision for clean data wiping shall be in the scope of contractor during dismantling as per owner's policy.**

z) All the cables required during entire process of shifting/re-shifting and installation of new system shall be in the scope of contractor.

aa) Additional Hardware, software and services necessary to ensure compatibility with existing equipment.
bb) CIM compliance and CIM database exchange

cc) Auditing of Cyber Security implementation and compliance by CERT-In Listed Auditors during FAT, SAT and AMC (bi-annually audit) as per Section 4 of Part-A. Every Bi-Annual Cyber Security Audit shall be conducted in phase-1 and phase-2, phase-1 initial audit (as per periodicity) and Phase-2 is follow up audit of phase-1 to check the closing of phase-1 audit observations. Phase-2 audit shall be conducted within 1 month of the phase-1 audit. The Contractor shall submit signed reports for phase-1 and phase-2 audits (signed by Certified Audit agency) to the Owner.

dd) Training Employer/Owner's personnel.

ee) Comprehensive Maintenance of the supplied system as per specification including future ICCP & RTU/SAS/Terminal server/DCPC Integrations, Database configurations, Maintaining Spare inventory etc. as deliberated in Section-4 Part-A of this specifications.

ff) During entire contract period (including extension of contract, if any), if OEM discontinues/ ends support to any item supplied (software/hardware/security solution) under the contract, contractor has to replace such hardware, software (or both, depending on software or hardware dependency) without any additional cost to Owner. Replacement shall be of either same or higher configuration and from same OEMs.

gg) Complete site overview display showing operating status of all hardware, LAN Wise Display in SCADA UI Browser along with alarms. The site overview display will also have provision for monitoring of historian functioning.

hh) Integration with other Applications: The SCADA/EMS System being supplied shall have provision to exchange data with other applications (existing and or to be purchased) such as Open Access Application, Scheduling application, WBES, Metering Applications, existing mail and SMS Alert systems of the Owner (RLDC/SLDCs) etc. SCADA/EMS System shall exchange data with these applications in standard API (Application Program Interface)/formats like SOAP, OPC, REST, ODBC, XML etc.

ii) GI/Aluminum cable trays/trace ways with covers shall be supplied by the bidder for laying cables so that cable can be protected from rodents. These cable trays/trace ways shall be screwed/ fixed on the floor by the contractor.

jj) Contractor shall supply necessary interface (Hardware and software) for sniffing/tapping the existing RTUs/SASs for parallel operation of new system with existing system.

kk) All the software licenses shall be in the name of the Respective Owner (Grid India for ERLDC and respective State Utility for SLDCs); License shall be purchased in the name of Owner (name of each location shall also be mentioned where these licenses will be deployed) and it shall be conveyed post award during Project Review Meetings (PRMs). Additional information e.g., Address, contact person, e-mail id, mob/land line number etc. for each CC location will also be provided by Owner. In the beginning of the Project, it should be informed to the Bidder by Employer/Owner in writing or as part of Kickoff meeting or PRM.

ll) Comprehensive AMC of complete system including supply of necessary interfaces (hardware and software) for integration of number of RTUs and Control Centers as specified in BOQ. All spare shall have pre-loaded software and required licenses in order to make it readily available for use at all times.

mm) Installation of new system at temporary location during parallel operation & shifting to final location, if required.

nn) Contractor shall supply necessary interface (hardware and software) for sniffing/tapping the existing SCADA/EMS system for parallel operation of new system with existing system.

oo) Signature updation throughout the contract period including AMC of various software licenses supplied under this project shall be in scope of the contractor.

pp) C10 Capacity test shall be done periodically (yearly), to determine whether the rating of battery is holding up using capacity test. If the battery capacity is less than 80% of its design value in any of the cases, the battery shall have to be replaced by contractor during entire period of contract (including extension of contract, if any) without any cost implications to owner. If number of cells replaced (cumulative) in battery bank exceeds more than 25% of total battery bank in any of the cases during entire period of contract (including extension of contract, if any), then contractor shall replace that entire battery bank without any additional cost to the Owner. Also, Refer Section 3 & Section 8 PART C of TS.

qq) Necessary support for providing Security Logs from Firewalls/Other Cyber Security Devices to NCIIPC and integration of supplied SCADA/EMS system with the future Security Operations Center (SOC) and Security Orchestration, Automation and Response (SOAR) systems to be procured by Owner(s).

rr) The contractor shall submit the undertaking as per format mentioned at Part-A, Appendix-K for all new items supplied under this project as well as any repaired items/components to certify that the items are free from embedded malware.

ss) **Annual OT security audit of supplied RTU under this project during entire AMC period as per cyber security guidelines issued by statutory authority and amended time to time shall be in the scope of the contractor.**

The above audit shall be carried out by following ISO 27019 along with other provision.

NOTE: All the scope of work defined for SLDC/RLDC under the proposed contract shall also be applicable for the Sub-SLDCs (if scope of Sub-SLDCs is envisaged) as per the proposed architecture, BOQ envisaged for Sub-SLDCs.

1.11 General Requirements

The Contractor is encouraged to offer standard products and designs. However, the Contractor must conform to the requirements and provide any special or additional equipment/s or software necessary to meet the requirements stated in the specification. It should be noted that preliminary design information and bill of quantity are minimum and indicative only; the Contractor shall verify jointly (with Employer/Owner) the design data during the site surveys & detail engineering and finalize the BOQ as required for ultimate design & system performance.

The Employer/owner reserves the right of execution of works within the stipulated quantity variation provision other than those indicated in the appendices at the same rates, terms and conditions.

The supplied system (hardware & software) shall comply with cyber security standard relevant clause of the Central Electricity Authority (Technical Standards for Communication System in Power System Operations) Regulations, 2020, Indian or International Security Standards e.g. IT and IT related elements against ISO/IEC 15408 standards, for Information Security Management System against ISO 27000 series Standards, IEC 62443 for OT Network Security, IEC 62351.

The procurement/bid proposal shall be compliant to these standards. The contractor shall ensure compliance with all the statutory guidelines issued during the entire period of contract from all the regulatory bodies. Before supply, the contractor shall certify the items for relevant cyber security standards. Certified auditors/CERT-In listed auditors for compliance to standards shall test the commissioned system under AMC. For ensuring compliance of cyber security standards, the contractor shall do Vulnerability Assessment and Penetration Testing (VAPT) & all patch management for complete life cycle of the project.

The Bidder's proposal shall address all functional and performance requirements within this specification and shall include sufficient information and supporting documentation in order to determine compliance with this specification without further necessity for enquiries. The Bidder's proposal shall clearly identify all features described in the specifications or in any supporting reference material thatwill not be implemented; otherwise, those features shall become binding as part of the final contract.

An analysis of the functional and performance requirements of this specification and/or site surveys, design, and engineering may lead the Contractor to conclude that additional items and services are required that are not specifically mentioned in this specification. The Contractor shall be responsible for providing at no addedcost to the Employer/Owner, all such additional items and services such that a viable and fully functional SCADA/EMS System is implemented that meets or exceeds the capacity, and performance requirements specified. Such materials and services shall be considered to be within the scope of the contract.

All equipment provided shall be designed to interface with existing equipment and shall be capable of supporting all present requirements and spare capacity requirements identified in this specification.

The equipment shall be designed and provisioned for expansions and reconfigurations without impairing normal operation, including adding and removing RTUs/channels & Control Centers. Adequate measures shall be taken to provide protection against rodents, contaminants, pollutants, water & moisture, lightning & short circuit, vibration and electromagnetic interference etc.

It shall be the employer's/Owner's choice to keep Furniture colour and design different for each Control Centre or same for all. Employer/Owner will choose option wherever an option of functionality is given. However, if 'or' is written then Supplier has to provide all the functionality. It can be explained by following example. Capability to export SCADA data to external system using ODBC or JDBC or OPC (ODBC/JDBC/OPC). In this case Supplier has to deliver all the three options to the user. **However, if 'or' OR '/' is mentioned in-lieu of certification/testing requirement for any of the items envisaged under the contract, in that case contractor has to meet minimum one requirement.** But if it is written that capability to export SCADA data to external system using either ODBC or JDBC then Supplier has to provide at least one option.

The Contractor shall demonstrate a specified level of performance of the offered items during well-structured factory and field tests. The contractor has to ensure during the entire contract period, if any supplied item (software and hardware including third party solutions/services) under the contract is discontinued / ends support/ is end-of-life, for all such items the contractor has to replace and provide the software/hardware/solution/service as per scope of technical specification without any additional cost to Employer/Owner.

The contractor has to provide solution/replacement either of same or higher configuration or from same OEMs without affecting the performance of the system with the approval of Employer/Owner. If any development, customizations, testing etc. needs to be done for the solution provided, then the same shall be borne by the contractor at its own cost during entire contract period **including extension of contract, if any.**

Contractor shall take care of all the cyber security audit recommendations from time-to-time throughout the life cycle of project.

The bidders are advised to visit sites (at their own expense), prior to the submissionof proposal, and make surveys and assessments as deemed necessary for proposal submission.

The successful bidder (Contractor) is required to visit sites and do site survey of all locations as per scope of the project. The site visits/routes shall include all necessary surveys to allow the contractor to perform the design and implementation functions. The Contractor shall inform their site survey schedule to the Employer/Owner well in advance. The site survey schedule shall be finalized in consultation with the Employer/Owner. The Employer/Owner may be associated with the Contractor during their site survey activities.

After the site survey the Contractor shall submit to the Employer/ Owner a survey report. This report shall include at least the following items:

a. Layout of all equipment (Server, Work Station, VPS etc.) in the rooms and buildings as required for final and intermediate positions.

b. Proposed routing of power, earthing, LAN cable and signal cables along with trench size at Control Center Locations to be supplied under this project.

c. Availability of Space, Air conditioning, Auxiliary Power Supply system including DG set and AC/DC Power supply

d. Proposals for new rooms/buildings/ trench/ facility modifications, if required

e. Identify all additional items required for integration for each site/location.

f. Survey report of field devices such as RTU, APS, DG set etc.

1.12 General Responsibilities and Obligations

This sub-section describes the general responsibilities and obligations of the Contractor and the Employer /Owner.

1.12.1 Responsibilities for the Implementation Plan

The contractor shall be responsible for development of detailed project implementation plan. The implementation plan shall include delivery of Hardware at Site, Data base development, Commissioning of new system, shifting of existing system, parallel operation of systems, shifting of new system to control room, Dismantling & migration of operations to the new system etc.
The Implementation plan shall include the activities of both the Contractor and the Employer/Owner, showing all key milestones such as facilities readiness and clearly identifying the nature of all information and project support expected from the Employer/Owner. In consultation with the Employer/Owner, Contractor shall finalize the detailed Implementation plan following award of the contract.

1.12.2 Contractor's Responsibilities and Obligations

The Contractor shall be responsible for all cabling and wiring associated with the equipment provided both inside and outside buildings. The Contractor shall also be responsible for determining the adequacy of the local power source for the equipment and for cabling to it, with adequate circuit protective breakers, if required.In addition, the Contractor shall be responsible for shielding equipment and cablingto eliminate potential interference to or from the equipment and for earthing of all cabinets and shields as required for system. Contractor's responsibilities include, but are not limited to, the following:

- Provide a working system that meets or exceeds the functional and performance requirements of this specification without affecting the operation of the existing systems.

- Provide a complete turnkey implementation and assume responsibility for all integration and implementation issues in order to deliver an operable system.

- To ensure the completion of the entire implementation within the scheduled time frame as mentioned in the tender fulfilling the entire tender terms and conditions.

- Site visits and studies necessary to identify and provide all equipment needed for implementation of the project.
- Equipment engineering and design specific to each location including review of, and conformance with local environmental and earthing considerations.
- All cabling wiring including supply, laying and termination of cables (signal, power supply & earthing), DC/AC distribution boards
- Development of installation guidelines and safety guidelines and procedures for the mechanical installation including testing and documentation.
- It is the responsibility of contractor to provide all the hardware and software to make the system fully functional as per technical specification
- Configure all features and functionalities in the network as indicated by the Employer/Owner during detail Engineering and implementation
- Overall integration of equipment/subsystem
- Integration of existing & new RTUs/SASs/Terminal Servers/DCPC
- Integration of existing & new Control Centers
- Integration of PDC and URTDSM System
- Integration of Renewable Energy Control Centre
- Integration of ICCP links envisaged in future with SCADA/EMS system during entire contract period of project and AMC (including extension of contract if any).
- Buying and maintaining of spares identified under AMC along with main items to meet the contingency during installation and Maintenance period.
- Project management, project scheduling, including periodic project reports documenting progress during the contract period.
- Engineering and technical assistance during the contract warranty and maintenance period.
- Provide all additional Equipment and services necessary to ensure compatibility between new and existing equipment.
- Implement all minor civil works and identify any major civil works i.e. expansion or construction of rooms, trenches necessary for installation ofproposed equipment and provide the details of such work to the Employer/Owner.
- Define source power requirements for each cabinet/ rack of equipment provided.
- All hardware, software, and firmware required to satisfy the requirements of this Specification.
- Supply, installation, testing and commissioning and AMC of all hardware, software, and firmware required to satisfy the requirementsof this Specification.

- Factory and site testing of all hardware and software provided.
- Provide Type Test report to the Employer/Owner and if required, conduct type test. The contractor shall submit type test reports for all the equipment as per specification for review & approval by Employer within 30 days of Contract Award. The type test reports submitted shall be of the tests conducted within last five (5) years prior to the date of bid opening. In case the test reports are older than five (5) years ago on the date of bid opening or the type test reports are not meeting the specification requirement, the contractor shall carry out the type testing at no additional cost to the employer.
- Testing for ICCP integration with the Existing system.
- Testing for integration of existing RTUs/SASs/terminal servers/DCPC
- Provide a Quality Assurance Plan and access to the manufacturing process.
- Shipment of all equipment to designated locations and/or storing areas.
- Storing, maintenance of storing area and security including full responsibility for protection from theft and fire for all the items to be supplied.
- All documentation and drawings as specified.
- All required spare parts, maintenance aids, and test equipment.
- Parallel operation of the existing and new system. However, the maintenance of the existing system will be responsibility of owner.
- Training of the Employer/Owner's personnel.
- Hardware, software, and firmware maintenance, debugging, and support of the equipment through final acceptance, and maintenance on all new equipment as per specifications.
- Periodically taking Full system backup of all installed software for all machines.
- Availability of service, spare and expansion parts for the supplied items for the complete design life i.e., during entire contract period (including extension of contract, if any) from the operational acceptance of the system of the project as per details in various parts of this specification. Contractor shall have back-to-back support & warranty from OEM only .
- Installation of new system at temporary location during parallel operation & shifting to final location, if required.
- Compliance of all applicable security related requirements as per latest DoT guidelines with subsequent amendments in the entire period of contract.
- All provisions and orders of **GOI, DPIIT, MoP, DoT, Meity etc. or any other Nodal Ministry** have to be mandatorily complied by the contractor with subsequent amendments in the entire period of contract **(including extension of contract, if any).**

Detailed descriptions of the Contractor's responsibilities, in relation to individual litems and services offered, are delineated in other sections of this specification.

1.12.3 Exclusions from Contractor's Scope

The contractor shall be responsible for providing all the hardware & software, development of database and services required for commissioning of the project except: -

- Buildings
- Air conditioning
- Firefighting system
- A.C. input power supply
- Communication System
- Auxiliary Power Supply for locations where it not included in the BOQs.

1.12.4 Owner's Responsibilities and Obligations

The Owner will provide the following items and services as part of this Project:

- AC Source power at (nominal) 3 phases 415V AC Power from two independent sources, where UPS included in the BOQs. At locations where it has not been included in the BOQs the 220V UPS Power supply shall be supplied by the Owner. However, the bidder shall submit the load details (In Amperes) for the equipment supplied by the contractor. Further, additional input source of DG Set for integration with APS shall also be provided where DG Set is not included.
- Any statutory clearance/ entry permits as required.
- Participation in "Type", factory and site acceptance tests.
- Power system network and device data
- Providing support and access to facilities at the sites.
- Implement the major civil works such as expansions or construction of rooms, trenches etc. as required for the equipment to be provided by the Contractor.
- Provide to the extent possible drawings for existing sites and facilities for which equipment installations are planned.
- Arranging appropriate shut down to facilitate erection testing and commissioning of System.
- Any statutory clearance/ entry permit as required.
- Owner will take over the RLDC/SLDC system upon completion of the project.
- Support during Maintenance Period
- AC in battery & UPS room
- **Communication system and link for data communication (RTUs to control**

centers and between control centers)

- **Internet connectivity of required bandwidth.**
- **Email Server.**

1.12.5 Employer's Responsibilities and Obligations

The Employer will provide the following items and services as part of this Project:

i. Overall project management.
ii. Review and approval of the Contractor's designs, drawings, and recommendations.
iii. Review and Approval of test procedures.
iv. Participation and Approval of "Type", factory and site acceptance tests.
v. Review and Approval of Training Plans.
vi. Review and Approval of Document Plan and Documents.
vii. Project review meeting with contractor.
viii. Coordination of the Contractor's activities with the Employer's concerned departments and Owner.

POWERGRID as the consultant shall also be responsible for all the above items and services on behalf of ERLDC except for the site activities.

1.13 Relocation and Commissioning at New Location (as per BOQ)

Owner may need to shift the entire set up (equipment/devices supplied under this project including integration of existing equipment, if any) to new location as detailed in BOQ - (Appendix-G PART-B) due to various reasons like renovation and modernization work etc., during entire contract period (including extension of contract, if any).

Following works shall be done during shifting the entire set up to new location:

- Dismantling of equipment's.
- Packing of dismantled hardware's.
- Unpacking of dismantled hardware at new location.
- Installation of all equipment including spares (if any) at new location.
- Integration, testing and validation at new location.
- Following are the contractor scope of work at control centre which is being shifted and other affected control centres (if any) during relocation and commissioning at New Location:
- Backup of all servers.
- Dismantling of all equipments.

- Marking / Tagging of all connected cables on equipments and removal of all cables with in the network and server panels/equipments.
- Packing of dismantled hardware.
- Unpacking of dismantled hardware at new control centre.
- Installation of all equipments at new control centre.
- Powering up of all equipment of dismantled equipment and spares at new control centres.
- Connection with Earth pit & Earthing till UPS room.
- Commissioning of installed hardware.
- Testing and integration of instrument/ test equipment.
- Project management.
- Technical management.
- **Integration, testing and validation at new location for RTUs, Control centers, other applications etc. The contractor shall not be including any RTU integration activities separately during relocation of items.**

The scope of work for relocation and commissioning at new location mentioned in Part-B, Appendix-G, Bill of Quantity is for once in the entire life cycle of the project.

Following are the **Owner** scope of work at control centre which is being shifted during Relocation and Commissioning at New Location:

- Transportation, Loading, unloading, F & I of dismantled hardware.
- Supply & Laying of Power Cables up to UPS (i.e., Utility Supply to UPS).
- Supply & Laying of Network Cables & Power Cables (UPS to SCADA System).
- Supply & Laying of Cables from Telecom Panel to SCADA Panel.
- Civil work including Trench extension, frame, supply of special tools and tackles etc. (as specified in Site Survey Report).
- Maintain Warehouse/ Store/ Security at Site.
- Statutory clearances.
- Air Conditioning.

1.14 System Architecture

The conceptual system architecture of Main and Backup Control Centers of RLDC/SLDCs i.e. Servers, devices and their interconnection at various Control

Centers is provided at Appendix-D of Part-A. The bidder can optimize and propose their own system architecture but shall meet functional requirement as well as future expandability, redundancy and the isolation required for cyber security.

1.15 Main and Backup Control Center Operational Philosophy

This specification document states the requirements for the SCADA/EMS systems, which the Contractor shall install at the main & backup control centers of RLDC/SLDCs. Apart from the number of workstations/servers associated with each system, the SCADA/EMS configurations shall be identical. The requirements stated in this document for "the SCADA/EMS", unless expressly indicated otherwise, shall apply equally to the SCADA/EMS Systems. Each SCADA/EMS shall be able to serve as a backup to the other system. In normal course, Main Control Center of the Constituents shall be performing all the functions of Main Control Center and Backup Control Center shall be functioning as standby to Main Control Center. Main Control Center shall update the Backup Control Center automatically. Main Control Center shall be primary Control Center for operations at all times, when available. The update/backup periodicity of data at Backup Control Center from Main Control Center shall be as follows:

- Real time data shall be updated every 10 second
- Historian data shall be updated every hour

In case of failure of the Main Control Center, the Backup Control Center shall takeover operations and functions of Main Control Center. When Main Control Center recovers from failure, Backup Control Center shall update all data, including Historian data (to be synced for user selectable period only) at Main Control Center or vice versa. The takeover of main Control Center functions by Backup Control Center shall not require manual intervention.

In case user required to sync data between main and backup control center historian for a selected period, it shall be possible.

Each SCADA/EMS shall be configured to communicate with the entire set of LDC's RTUs/SAS/terminal servers and Control Centres and shall have the database and full set of displays & reports for the entire region. If communication with data source is available with one Control Center (say main Control Center) and not with other Control Center (Say Backup Control Center) then other Control Center data shall be updated by the first Control Center which has updated values e.g. a SLDC and a RTU communication link is failed with main RLDC but communication link with backup RLDC is healthy and backup RLDC is getting data from these sources. Then Main RLDC shall get data from Backup RLDC for these sites (SLDCs and RTUs) automatically and vice versa.

1.16 General Bidding Requirements

The Bidder shall be responsive to the Employer's/Owner's technical requirements as set forthin this specification. To be considered responsive, the Bidder's proposal shall include the following:

- The Technical Proposal including the documents listed in the Table 1-1: Bid Documents Checklist shall be provided in the bid,
- A detailed project implementation plan and schedule that is consistent with Employer's specified objectives. The plan shall include the activities of both the Contractor and Employer/Owner, show all key milestones, and clearly identify the nature of all information and project support to be provided byEmployer/Owner.
- A System description Document describing the overview of bidder's proposed Software and Hardware System.
- A commitment and a clearly defined plan to develop a system support organization, based in India and capable of providing a full range of local Services (including software and hardware maintenance and upgrade support) for the life of the delivered systems.
- The migration plan detailing the minimum space and logistics requirementat existing Control Center, parallel operation of the existing system for 3 Months without disturbing the operation of the existing system, Expected downtime in existing system, dismantling of the existing system and shifting the operation to the new system.

The bidder shall submit the power consumption details of each RLDC/SLDCs system.

Table 1-1

Bid Documents Checklist

S.No	Description	Enclosure	Reference
1	Completed Data Requirement Sheets (As per relevant sections of Technical Specification)	Page no.	Ref No.
2	System description Document	Page No.	Ref. No
3	System Capability, including data sizing and Upgrading Capabilities (As per relevant Sections of Technical Specs Volume II)	Page no.	Ref no.
4	Schematic Diagram of Proposed System Configuration for each Constituent.	Page no.	Ref no.
5	Quality Assurance Program (As per relevant Sections of Technical Specs Volume II)	Page no.	Ref no.

6	Detailed Project Implementation Plan (As per relevant Sections of Technical Specs Volume II)	Page no.	Ref no.
7	A migration plan from the existing system to the new system for each Constituent (RLDC/SLDCs) without affecting the operation	Page No.	Ref No.
8	Answers to **Appendix-E of part-B** Questionnaire	Page No.	Ref No.

1.17 Applicable Standards

The applicable standards are mentioned in the respective technical section. The offered equipment shall conform to the standards mentioned in the specification except to the extent modified by this specification, if any. In case of any discrepancy between the description given in the specification and the standards the provisions of the technical specification shall be followed unless specifically agreed to during bidding process.

The available equivalent Indian Standard shall be complied. All latest guidelines issued by regulatory authorities such as **MoP CEA, NCIIPC, MEITY etc. shall be complied by the bidders for the offered products (hardware and software) under the project. These should be established and tested product (hardware and software) considering criticality of the system.In this regard, bidder has to comply with order issued by MoP No. 25-11/6/2018-PG dated 2.7.2020 (with all amendments) and CEA Cyber Security in Power System Guidelines, 2021 (with all amendments) throughout the period of contract.**

Specifications and codes shall be the latest & Proven/tested version, inclusive of revisions, which are in force. Where new specifications, codes, and revisions are issued during the period of the contract, the Contractor shall attempt to comply with such, provided that no additional expenses are charged to Employer/ Owner.

In the event the Contractor offers to supply material and/or equipment in compliance to any standard other than those listed herein, the Contractor shall provide, salient characteristics of the proposed standard for comparison. The Employer/Owner will assess the merit of material/equipment and will be sole judge as to their acceptance.

1.18 Table of Compliance

Bidder shall use one copy of Volume I, "Conditions of Contract" and Volume II, "Technical Specifications" to indicate compliance status and Technical Status with those volumes.

Within the right-hand margin, Bidder shall indicate compliance status and technical Status to each paragraph and an index key for any explanation or comment. In addition, the Bidder shall annotate the Table of Contents of each of the above stated volumes to provide a high-level summary of compliance status and Technical Status.

In both cases, the following symbols, and no others, shall be used.

Compliance Status: -

C Bid complies with all requirements

A Bid is not compliant with the requirements, but a functional alternative is proposed.

X Bid takes exception to the requirements and no functional alternative is proposed.

Technical Status: -

S Bidder's Standard product will be used to meet the Requirements

D Bidder will take development work to meet the Requirements

Only one symbol of Compliance Status and one symbol of Technical Status shall be assigned for a paragraph and shall indicate the worst-case level of compliance for that paragraph. This annotation may be handwritten.

Bidder shall also underline, on the compliance copy, all requirements to which exceptions have been taken (X) or to which alternatives have been proposed (A). Each alternative shall be clearly and explicitly described. Such descriptions shall use the same paragraph numbering as the bid document sections addressed by the alternatives. All alternative descriptions shall be in one contiguous section of the

Bidder's proposal, preferably in the same volume, and titled "Alternatives."

A separate section titled "Exceptions" should be provided containing any discussion or explanation Bidder chooses to provide concerning exceptions taken.

Alternatives which do not substantially comply with the intent of the bid documents will be considered exceptions.

The Employer/Owner will assess the merits of each alternative and exception and will be the sole judge as to their acceptance.

-----------------End of the Section1-------------------

Section-2

Training

Table of Contents

Section 2 Training

2.0 Introduction

This section describes the project requirements for Employer/Owner's Personnel Training. All Training material and presentation shall be prepared in line with project design/solution. Training material and presentations should be approved by the employer prior to imparting conduct training sessions.

2.1 Training

- Training shall be conducted by Contractor personnel who are experienced instructors and speak understandable English.
- All necessary training material shall be provided by the Contractor. Each traineeshall receive individual copies of all technical manuals and all other documentsused for training.
- Class materials, including the documents provided to the trainees as well as class handouts, shall become the property of Employer/Owner. Employer/Owner reserves the right to copy such materials, but for in-house training and use only.
- Hands-on training shall utilize equipment similar to that being supplied under thecontract. In general training duration shall be 50% for hands on except databaseand dispatcher which could go up to 80% for hands on training.
- The Bidder shall include a description of the Bidder's proposed organization and administration for implementation of the training program, indicating the responsibility for training within the Bidder's proposed site organization and home office organization and indicating the staff responsible for the various components of the training. Training modules for various users and various administrators are to be prepared in consultation with employer/owner.
- For each course, detailed learning objectives must be developed and specified, based on the course objective. The detailed learning objectives must state what the trainee should be able to do as a result of the training. When detailed learning objectives have been defined, the contents of the training must be designed to provide the learning experience which will enable the trainees to reach the learning objectives.
- The contractor shall provide rigorous training to be made for each module. The contractor shall be responsible to train the operator in every field, whether it is system software, application software, cyber security, hardware, APS, VC, RTU etc.
- For all training courses the travel (e.g., airfare, rail fare, and road transport etc.) and daily expenses for the participants (not contractor) will be borne by the Owner. For courses conducted abroad, however, the Contractor shall

extend all necessary assistance for making appropriate lodging arrangements.

- The Contractor shall quote training prices individually for each of the courses as per Table given below.
- The schedule, location, detailed contents and batches for training for each course shall be finalized during detail engineering. The number of participants in the training program may undergo change.
- Employer/Owner will have the option to cancel any or all training courses. In the case of cancellation, the rate quoted against the respective course will not be paid to the Contractor.
- For training at site, the Employer/Owner will provide Conference room and facilities however any specific training tool/manual/test paper/exercise and stationery shall be provided by the Contractor
- No later than one month after the Commencement Date, the Contractor shall submit for approval by the owner/employer, a detailed training plan reflecting the actual courses to be conducted by the Contractor. Owner will have the option to shift / avail any or all training courses (part or full) from project execution period to AMC period, if total envisaged man-weeks of the training not availed during completion of project due to unavoidable circumstances. The rate quoted against courses will be paid to the Contractor as per actual usage.
- 3rd party Supplied Software Training shall be involved with respective OEMs/authorized partners.

The training courses, their duration, and the number of employer/owner's personnel to be trained in each course are identified in **Table given below.**

2.2 Introduction to RLDC/SLDCs Operation Course

This course shall provide basic knowledge on the RLDC/SLDCs Project and the new RLDC/SLDCs System itself. It shall be held immediately after installation of the Development System components and shall be held in the form of instructor directed lessons and demonstrations. This course shall cover the following concepts.

a) Project scope and schedule

b) Use of operator consoles

c) Usage of the RLDC/SLDCs specific Software modules

d) Basic process control functions

e) Basic HMI functions

f) Video Projection System

g) Principles of display design

h) Dialog procedures

i) Historical data storage, presentation and report generation

j) Analysis of Alarms

2.2.1 Training Requirement for SCADA/EMS and HISTORIAN System

Employer/Owner training course requirements are described below in terms of the contentsof each course to be provided. Training shall be provided on supplied system database for the application software course, database and display building, the dispatcher training course and the associate training courses.

2.2.1.1 Database and Display Building Course

The database and display building course shall be the first course to be given in the overall training sequence. It shall be primarily a hands-on course. The course shall be designed to train Employer's/Owner's personnel in how to develop the databases, displays, reports and configure alarms, events, logs etc. for the supplied system.

Course objectives shall include:

- How to identify database fields, entries, records (to be managed by DB Tool automatically), tables and contents.
- How to build tables, arrays and report formats.
- How to build displays.
- How to perform database maintenance.
- How to generate the database from source information.
- How to maintain symbol libraries, display colour groups and display string lists.
- How to Track and reverse database changes.
- How to do Online editing of Databases and Displays.
- How to generate reports using database queries and web services.
- How to define SCADA, ICCP, FEP, EMS and AGC databases.
- How to create calculations using scientific functions. Creation of functions as per user requirement for database calculations.

On course completion, all participants shall be able to prepare the necessary input data to define the system operating environment, build the system database and displays and prepare the database administrator to maintain and modify the database and its structures. This will include the database modelling and population for neighboring systems also.

The database maintenance personnel shall actively participate in data migration for the new RLDC/SLDCs and shall supervise the database population, display and report generation for integration of newly built stations into the RLDC/SLDCs SCADA system by contractor.

2.2.1.2 Computer System Hardware and Software Course

The training course shall be designed to give Employer/Owner personnel sufficient knowledge of the overall design and operation of the system so that they can correct the problems, configure the hardware, perform preventive maintenance, run diagnostic programs and communicate with contract maintenance personnel. This training shall provide the RLDC/SLDCs personnel with in-depth knowledge about the control system design, hardware configuration, individual computers, operator workstations and peripherals. In addition to these training, there should be active participation in installation, commissioning and acceptance testing of all equipment.

The following subjects shall becovered:

(a) System Hardware Overview: Configuration of the system hardware. Preventivemaintenance techniques and diagnostic procedures for each element of the computer system, e.g., processors, auxiliary memories, LANs, routers, firewall, IPS, IDS and printers. Basic components of control systems as processor, memory, I/O units, graphic adapters LAN and communication controllers, etc. Peripherals (printers, hardcopy, tape units, terminal servers, large screen projection etc.), Installation procedures & Server monitoring.

(b) System Expansion: Techniques and procedures to expand and add equipmentsuch as memory in server, printer, communication channels, router ports, workstations and Control Centres. This shall also include adding New RTUs and newControl Centres.

(c) System Configuration: Procedures of configuring Router ports, VLANs, FirewallPolicy definitions and Interfacing web services.

(d) System Maintenance: Basics of operation and maintenance of the redundant hardware configuration, fail over hardware, failure of Control Centres configuration control panels and fail over switches. Maintenance of protective devices and power supplies. Hardware and software tools for fault diagnosis, Equipment/module replacement procedures and Equipment/module restart procedures

(e) Subsystem Maintenance: Theory of design and operation, maintenance techniques and practices, diagnostic procedures and (where applicable) expansion techniques and procedures. Classes shall include hands-on trainingfor the specific subsystems that are part of supplied systems. All interfaces to the computing equipment shall be covered in detail.

(f) Operational Training: Practical training on preventive and corrective maintenance of all equipment, including use of special tools and instruments. This training shall be provided on supplied equipment, or on similarly configuredsystems.

(g) System Programming: An introduction to software architecture, Effect of tuning/configuration parameters (OS software, System Software, Application Software, Network software, database software, firewall, IPS antivirus etc.) on the performance of the system, Administration of Database (both real-time and RDBMS, security).

(h) SCADA & EMS: Hands–on training on SCADA and EMS applications shall be provided along with user interface and covering all the functionalities in details. Training of EMS shall cover all the modules of EMS in details.

(i) Operating System: Including the user aspects of the operating system, such as program loading and integrating procedures; scheduling, management, service and utility functions; and system expansion techniques and procedures.

(j) System Initialization and Failover: Cold setup, warm setup Including design, theory of operation and practice

(k) Operation between Main & Backup Control Centre.

(l) Diagnostics: Including the execution of diagnostic procedures and the interpretation of diagnostic outputs.

(m) Software Documentation: Orientation in the organization and use of system software documentation.

(n) Hands-on Training: One week, with allocated computer time for trainee performance of unstructured exercises and with the course instructor availablefor assistance as necessary. Hands-on on at least 3 servers i.e. SCADA/EMS, FEP, ICCP etc., for the installation of operating system, application software's configuration shall be provided.

(o) System hardening and Cyber security: **All modules of Cyber security shall be covered in details which as a minimum include GUI, log filtering & searching, reporting, configuration changes, addition/deletion of new rules/policies/devices etc.**

2.2.1.3 Application Software Course

The Contractor shall provide a comprehensive application software courses covering all applications. The training shall include:

2.2.1.3.1 SCADA:

(a) Overview: Block diagrams of the application software and data flows.Programming standards and program interface conventions.

(b) Application Functions: Functional capabilities, configuration, associated maintenance and expansion techniques.

(c) Software & Protocol Administration: Techniques and conventions to be used for the preparation and integration of new software functions including Application Program Interface (API) interfaces and Web services. It shall also include the configuration/modification of software to integrate a new RTU/Terminal server and a Control Centre. This shall also include configuration of system for IEC 60870-5-101, IEC 60870-5-104, ICCP, Security (IEC 62351), CIM (IEC 61970), Web services, OPC and other Standards specified in the Specification.

(d) Software Documentation: Orientation in the organization and use of functional anddetailed design documentation and of programmer and user manuals.

(e) Cyber security related features of application e.g. user authentication, encryptionetc.

2.2.1.3.2 EMS

(a) EMS Applications: All PSA applications of EMS to be covered along with its integration with PMU and various databases along with all functionalities.

(b) Automatic Generation Control (AGC): Control Area wise configuration and Mode of operations of AGC to be covered along with all functionalities.

(c) Dynamic Security Assessment (DSA): Creation of dynamic models for DSA and its integration with EMS snapshot and for base case initialization along with all functionalities.

2.2.1.4 Historian System Course

The Historian System training course and documentation shall impart comprehensive training and information on the structure of Historian Database, details of all database tables and their fields, procedures and sub-routines being called to populate the database tables etc. On completion of the course, the trainees shall be able to customize the Historian Database, create their own database tables and shall be able to create new procedures/sub-routines and call pre-written procedures/sub-routines to automatically populate the new tables with SCADA data. The Course shall also provide comprehensive training on the forms, reports and displays etc., provided by the contractor in the Historian System. The training shall also cover tools being supplied by the contractor to generate database forms, reports and displays etc. On completion of the training, the trainees shall be able to manage the existing forms, reports and displays as well as generate new forms, reports & displays etc., as per their own requirement using the data stored in Historian System.

2.2.1.5 Dispatcher Training Course

This training course shall provide SCADA/EMS training for employer/owner dispatchers. Emphasis shall be placed on application of system to monitor and control power system. Employer/owner anticipates that this training will be a combination of group and individual sessions at the control centre sites. During individual sessions, the course instructor shall work with one dispatcher only. The Training shall include System Overview, General Operating Procedures, System Applications, Handling of Equipment and Dispatcher Documentation. The course shall focus on hands-on training on the system. The trainees shall perform instructor-defined procedures with the help of the dispatcher documentation.

Training shall include updating of base case and profiles (load and generator both) for user selectable time range. Configuration of dynamic models for thermal, hydro and renewable generator sources so as to enable the user to replicate its power system dynamics in DTS.

The training shall primarily be used to acquaint the trainees with the functions of the instructor of the Dispatcher Training Simulator (DTS). This should include but not be limited to configuration of different scenarios such as Black Start, System Islanding, Voltage Collapse etc. on training simulator to be performed by instructor, configuration of DTS parameters, maintenance of DTS database and modeling, scenario to be created for users, how to interrupt and help the trainees to utilize the full functionality of DTS.

2.2.1.6 Network Management System Course

The NMS training shall familiarize the Employer's/Owner's maintenance personnel with the concept and techniques for configuring, programming, maintaining, and troubleshooting the Contractor supplied NMS and its associated database and services.

The Contractor shall train the Employer's/Owner's personnel who will operate the communications network, in the functional capabilities of the networking equipment. Each course shall provide a thorough understanding of the general design concepts, features, and user interface requirements for local and remote monitoring of the equipment, as well as procedures for restoring service after equipment and power failures. Each course shall include hands-on training using the actual hardware and software being delivered to the Owner.

Training aids for each course shall include the Operator's User Manual for each type of equipment. Operator training that is a standard part of the maintenance training will be applicable. The minimal NMS Training requirements are:

- Features of the software being supplied.
- System configuration procedures, including operating system & database parameterization and buffer sizes.
- Operating system concepts, including resource allocation, priority level processing, performance monitoring, diagnostic messages, and restoration procedures.
- Concepts and techniques for creating, modifying, and saving database, displays,and reports.
- Creation and Modification for display and reports for Channel monitoring of RTUlinks and ICCP Communications.
- Integration, configuration and monitoring of new devices/nodes in the NMS.

2.2.1.7 Cyber Security Course

The Contractor shall provide a comprehensive training on 'Cyber Security' to the system administrators of the Owner/Employer. The training shall familiarize the Owner's/Employer personnel with the basic understanding of network architecture, cyber security concepts, possible threats & vulnerabilities of the system, effective configuration of the network control elements and recovery management. The training on Cyber Security shall cover the following concepts.

- Access controls
- Device configuration
- Anti-virus/patch management
- Password management
- Knowledge on remote administration
- Incidence response
- Disaster recovery
- Awareness of Cyber security standards
- Monitoring for Critical Infrastructure Protection
- Compliance manager for Critical Infrastructure Protection
- Event log/Syslog analysis
- Firewall policy definitions
- Security Certificate and management
- SIEM
- Identity Management
- NIPS, HIPS and HIDS
- Network/port scanning and port management (opening and blocking of ports)
- Log monitoring and management
- Vulnerability Assessment and Penetration Testing (VAPT) procedure
- **Tools such as application whitelisting, VAPT etc**.

2.2.1.8 Training Requirement for Auxiliary Power Supply

The training shall focus on various aspects associated with Design, installation, testing & commissioning of UPS system that prepares personnel for on-site operation and maintenance of all equipment being supplied including automatic shutdown of Servers, Workstation and VPS. The training course shall include:-

- System design and overview,

Diagnostic and maintenance.

- Installation and operation mode.

Proper emphasis of the training shall be on effective monitoring, operation & maintenance of Auxiliary Power Supply System on routine and emergency basis by the personnel.

2.2.1.9 RTU/ Terminal Server/DCPC Course /ICCP Course

The Contractor shall provide an RTU/Terminal Server/DCPC/ICCP course that covers the followingsubjects as a minimum:

- Interface, interaction and operation of all RTU/ Terminal Server functional as well as physical blocks e.g. CPU/AI /DI/power supply/Communication interface etc.
- Operational procedures for various modes of operation, including diagnostic tests and interpretation of the associated test results.
- Implementing and maintaining multiple communication ports.
- Converting an RTU/ Terminal Server from one protocol to a different protocol.
- Demonstration of complete RTU/ Terminal Server test set use, including test set connection and set up for all possible modes of operation, all operational procedures, the exercise of each command or feature associated with each mode of operation, the interpretation of results and how to use the test set to diagnose and isolate RTU/ Terminal Server problems.
- Diagnostics for isolation of failure/fault in RTU/ Terminal Server/DCPC, earthing, system interface cabinet (SIC), Cabling, meters.
- Configuring all options on RTU/ Terminal Server protocol interface with master stations and configuring all parameters of MFTs.

The Contractor shall provide an ICCP course that covers the following subjects as a minimum: -

1. Configuration of ICCP association and integration with new control center.
2. Configuration of Secure & Non-Secure ICCP association.
3. Diagnostics of ICCP association, rectifying/ identifying ICCP problem.
4. Implementing conversion tables for individual ICCP associations.

2.3. Training Plan

Contractor shall propose a plan for implementation of the Training Program. The plan shall describe the sequencing, time, duration and resources involved in implementation of each of the contractor's proposed training activities. The plan shall be illustrated by a bar chart or diagram with the Work Plan and Staffing Schedule for the Training Program, indicating timing and staff responsible for the various training components. To demonstrate the relation between the overall plans for training, the contractor shall present the training activities in a bar chart, where the other project activities are also presented.

2.4. Training Manuals

Two types of training manuals are required for each course. A Trainer Manual will serve as a guide to the trainer and therefore, contain all necessary guidance and materials to

plan and implement the course. A Participant Manual will serve as guidance for each trainee, and thus include all necessary material (e.g. reading materials, hand-outs, exercises) to be handed out during the course.
The two training manuals must be prepared for each of the courses (whether classroom based or On-the-job) to be conducted. Not later than one month before start of a course, the Contractor will submit a draft of the Trainer Manual for approval of the Owners' administration. The two training manuals must be presented in ring binders and be of a good quality in terms of printing and English language usage. It must be clear from the Trainer Manual which material will be inserted in the Participant Manual.

Within the framework of the approved Course Description the Trainer Manual will provide, in the form of lesson plans, a detailed description of the sequencing of the training in the various subjects and work tasks. The Trainer Manual will contain the following:

- Course Description
- Course Program
- Lesson Plans
- Lesson title
- Lesson objectives
- Duration
- Teaching method(s)
- Trainer(s)
- Reading materials and hand-outs
- List of facilities and equipment required
- Exercises to be carried out
- Trainee assessments/tests

If, during the implementation the Contractor finds that training in some subjects is more demanding and time consuming than anticipated, the Contractor shall propose appropriate revision of Course Descriptions and Lesson Plans to the Owners' administration. The training manuals shall be amended by the Contractor according to any revisions of the training, so that they reflect the training which has actually been carried out. After taking over, the Trainer Manuals will be handed over to Owners to support Owners' training activities in the future. All the soft copy of the training manuals and training material shall be provided to the owner. The Contractor must produce manuals for operation and maintenance of the works delivered under the contract.

2.5. Quality Assurance of Training

2.5.1. The Contractor's Trainers

The Contractor may choose to delegate the responsibility for preparing and conducting training courses between his own site and home office staff; training specialists of sub-contractors and original equipment manufacturers, as found appropriate. The overall responsibility for the training remains with the Contractor and the training organization and quality assurance procedures must reflect the following details:

The training staff must have the following qualifications:

- Experience in training of staff with background comparable to that of the RLDC/SLDCs trainees.
- Basic understanding of learning and motivational theory and practice.
- Experience in preparation of instruction materials and manuals.
- Basic communication skills.
- Education and work experience relevant to the subjects covered by the training in question.

It shall be noted that candidates proposed as trainers must not only have the required technical qualifications but also qualifications within the teaching/training field. The Contractor shall document the experience of the proposed training staff by inclusion of CVs. The Training Plan of the Contractor must clearly indicate the area of responsibility and timing of input of all training staff. It shall be noted that proposals of staff to be responsible for project tasks and training tasks at the same time will not be accepted.

2.6 Training facilities and equipment

Owner will arrange a room for the Contractor in India, furnished with chairs and tables.

In the bid, the bidder shall include equipment to carry out training, including items such as beamer, white boards, video equipment, photo copying machine, document binder, and all such training equipment, tools and materials as will be required specifically for classroom as well as on-the-job training. Bidders shall list the equipment and provide respective technical data with their offer.

2.7 Records

The Contractor shall keep a record of all training, records of participation in training.

2.8 Yearly training under AMC

The contractor shall be responsible for providing yearly training on complete system for 5 Days for 20 owner's personnel and 10 Employer's personnel during entire period of project.

Table:2.1 – Training Requirements

S. No.	Description	No of trainees to be trained for each RLDC/SLDC								Total No. of Trainees	Duration in weeks		Total Man-weeks	
		ERLDC	DVC	WBSE TCL	OPTCL	BSPTCL	JUSNL	SIKKIM	Employer		At Contractor's facility	At Owner's facility	At Contractor's facility	At Owner's facility
1	Computer System Hardware &Software	6	5	5	5	5	5	5	2	38	2	2	76	76
2	Database & Display	6	4	4	4	4	4	4	2	32	2	3	64	96
3	Application Software	26	5	5	5	5	5	5	2	58	3	4	174	232
4	Training to Dispatcher/Operator	10	12	12	12	12	12	12	2	84	2	3	168	252
5	Training on NMS	3	2	2	2	2	2	2	2	17	1	1	17	17
6	Cyber Security	8	4	4	4	4	4	4	2	34	2	2	68	68
7	Dispatcher Training Simulator	4	4	4	4	4	4	4	2	30	2	3	60	90
8	RTU	0	0	0	0	0	4	4	2	10	1	1	10	10
9	Terminal Server/DCPC/ICCP Course	6	5	5	5	5	5	5	2	38	1	1	38	38
10	Aux.Power Supply	4	4	4	4	4	4	4	2	30	0	1	0	30
	Total	**73**	**45**	**45**	**45**	**45**	**49**	**49**	**20**	**371**	**16**	**21**	**675**	**909**

One Man-week = 5 working days

NOTE:

1. Contractor shall facilitate site training at Owners MCC and BCC site as per Owner's requirement.

2. Number of trainees may vary as per the requirement of Owner for any module, payment shall be released accordingly as per the actual utilization for each module.

------End of Section 2------

SECTION 3

PROJECT MANAGEMENT, TESTING AND DOCUMENTATION

Table of Contents

Section 3 Project Management, Testing and Documentation

3.1 Introduction

This section describes the project management, schedule, quality assurance, and documentation requirements for the project.

3.2 Project Management

The Contractor shall assign a Project Manager with the authority to make commitments and decisions that are binding on the Contractor. Employer will designate a Project Manager to coordinate all Employer project activities. All communications between Employer and the Contractor shall be coordinated through the Project Managers. The Project Managers shall also be responsible for all communications between other members of the project staffs including sub- contractor, if any.

3.3 Project Schedule

The project implementation plan is as given in Appendix-E of Part-A. Based upon this the bidder shall submit a preliminary project implementation schedule along with the bid. The detail project implementation schedule shall be submitted by the Contractor after award for Employer's approval, which shall include at least the following activities:

(a) Site Survey

(b) Testing at Site for interface with existing RTUs/SASs/terminal Servers/DCPC and Control Centers

(c) Migration Plan from existing to new Control Centre

(d) Documents, DRS, Drawing submission and approval

(e) Database development, Display and Report development

(f) Type Testing

(g) RTU Dispatch and Installation

(h) Hardware purchases, development/manufacturing and integration

(i) Dispatch

(j) Receipt, Storage, Installation & Field update schedule

(k) Factory & Site Testing Schedule

(l) Training schedule

The project implementation schedule shall include the estimated period for completion and its linkage with other activities. The Project implementation schedule shall also contain Employer activities required for the Contractor to complete the system.

3.4 Progress Report

A progress report shall be prepared by the Contractor each month against the activities listed in the project schedule. The report shall be made available to Employer on a monthly basis, e.g., the 10th of each month. The progress report shall include all the completed, ongoing and scheduled activities and transmittals issued and received for the month.

3.5 Transmittals

Every document, letter, progress report, change order, and any other written transmissions exchanged between the Contractor and Employer shall be assigned a unique transmittal number. The Contractor shall maintain a correspondence index and assign transmittal numbers consecutively for all Contractor documents.Employer will maintain a similar correspondence numbering scheme identifying documents and correspondence that Employer initiates.

3.6 Review Meetings

Progress meetings shall be scheduled by the Project Manager and attended by the Contractor and Employer to review progress of the project. Progress meetings shall be used to review the progress report, written correspondence exchanged since the last meeting, and open action items.

The Contractor shall also attend technical meetings as required to discuss technical aspects of the project and to review Employer comments on approval documents. When appropriate, these technical meetings shall be conducted as extensions to the progress meetings.

Contractor shall also attend the special meetings being conducted by respective Regional Power Committees for SCADA/Telemetry purposes if required.

3.7 Testing

This section describes general requirement applicable to all type of equipment being supplied under the project. For System and Equipment specific requirements are given in respective parts of the specifications.

3.7.1 Quality Assurance & Testing

All materials **(hardware, software etc.)** and parts of the system/sub-system to be supplied under the project shall be of **reputed** manufacturer from a supplier regularly engaged in the production of such equipment and producing such components since last five years at-least.

3.7.2 Quality Assurance and Quality Control Program

The Contractor shall maintain a Quality Assurance/Quality Control (QA/QC) program that provides that equipment, materials and services under this specification whether manufactured, designed or performed within the Contractor'splant, in the field, or at any sub-contractor source shall be controlled at all points necessary to assure conformance to contractual requirements.

The program shall provide for prevention and ready detection of discrepancies and for timely and positive corrective action. The Contractor shall make objective evidence of quality conformance readily available to the Employer. Instructions and records for qualityassurance shall be controlled and maintained at the system levels. Contractor shall describe his QA/QC program in the Technical Proposal, (along with samples from his QA/QC manual) and shall submit his QA/QC Manual for review and acceptanceby the Employer.

Such QA/QC program shall be outlined by the Contractor and shall be finally accepted by Employer after discussions before the award of Contract. A Quality Assurance Program of the Contractor shall generally cover but not be limited to the following: The organization structure for the management and implementation of theproposed Quality Assurance Program.

- The organization structure for the management and implementation of the proposed Quality Assurance Program
- Documentation control system.
- Qualification data for key personnel.
- The procedure for purchase of materials, parts/components and selection of sub-contractor's services including vendor analysis, source inspection, incoming raw material inspection, verification of material purchases, etc.
- System for shop manufacturing including process controls.
- Control of non-conforming items and system for corrective action.
- Control of calibration and testing of measuring and testing equipment.
- Inspection and test procedure for manufacture.
- System for indication and appraisal of inspection status.
- System for quality audits.
- System for authorizing release of manufactured product.
- System for maintenance of records.
- System for handling, storage and delivery.
- A Quality Plan detailing out the specific quality control procedure adopted for controlling the quality characteristics of the product.

The Quality Plan shall be mutually discussed and approved by the Employer/Owner after incorporating necessary corrections by the Contractor as may be required.

Neither the enforcement of QA/QC procedures nor the correction of work mandated by those procedures shall be cause for an excusable delay. An effectiveQuality Assurance and Quality Control organization shall be maintained by the Contractor for at least the duration of this Contract.

The personnel performing QA/QC functions shall have well- defined responsibility, authority, and organizational freedom to identify and evaluate quality problems and to initiate, recommend, or provide solutions during all phases of the Contract. The QA/QC organization of the Contractor shall be an independent administrative and functional structure reporting via its manager to the Contractor's top management.

The QA/QC manager(s) shall have the authority within the delegated areas of responsibility to resolve all matters pertaining to quality to the satisfaction of Employer when actual quality deviates from that stated in the Work Statement.

The Contractor shall be required to submit all the Quality Assurance Documents as stipulated in the Quality Plan at the time of Employer's inspection of equipment/materials. The Employer or his duly authorized representative reserves the right to carryout Quality Audit and Quality Surveillance of the systems and procedures of the Contractor's/his vendor's Quality Management and Control Activities. The scope of the duties of the Employer, pursuant to the Contract, will include but not be limited to the following:

(a) Review of all the Contractor's drawings, engineering data etc.

(b) Witness or authorize his representative to witness tests at the manufacturer's works or at site, or at any place where work is performed under the Contract.

(c) Inspect, accept or reject any equipment, material and work under the Contract in accordance with the specifications.

(d) Issue certificate of acceptance and/or progressive payment and final payment certificate.

(e) Review and suggest modification and improvement in completion schedules from time to time; and

(f) Monitor the Quality Assurance program implementation at all stages of the works.

3.7.3 Inspection Certificate

The Contractor shall give the Employer two weeks in case of domestic supplies and six weeks in case of foreign supplies written notice of any material being ready for testing. Cost incurred on such tests shall be to the Contractor's account exceptfor the expenses of the Inspector.

The Employer, unless witnessing of the tests is waived, will attend such tests on the scheduled date for which Employer has beenso notified or on a mutually agreed alternative date. If Employer fails to attend thetesting on the mutually agreed date, Contractor may proceed with the test which shall be deemed to have been made in the

Inspector's presence and Contractor shall forthwith forward to the Inspector, duly certified copies of the test results in triplicate. The Employer shall, within fourteen (14) days from the date of inspection as defined herein, give notice in writing to the Contractor of any objection to any drawings and all or any equipment and workmanship which in his opinion is not inaccordance with the Contract.

The Contractor shall give due consideration to suchobjections and shall make the modifications that may be necessary to meet said objections. When the factory tests have been completed successfully at the Contractor's or Sub-contractor's works, the Employer shall issue a certificate to thiseffect within fourteen (14) days after submission of such report by the Contractor after completion of tests but if the tests are not witnessed by the Employer, the certificate shall be issued within fourteen (14) days of receipt of the Contractor's Test Certificate by the Employer.

The completion of these tests or the issue of the certificates shall not bind the Employer to accept the equipment should it, on further tests after erection, be found not to comply the Contract on further tests after Erection. In cases where the Contractor provides for tests, whether at the premises or works of the Contractor or of any Sub-contractor, the Contractor except where otherwise specified shall provide free of charge items such as labor, materials, electricity, fuel, water stores, apparatus and instruments, as may be reasonably demanded by the Employer or his authorized representative to carry out effectively such tests of the equipment in accordance with the Contract and shall provide facilities to theEmployer or his authorized representative to accomplish testing.

The inspection by Employer and issue of Inspection Certificate thereon, shall in noway limit the liabilities and responsibilities of the Contractor in respect of the agreedQuality Assurance Program forming a part of the Contract. The Contractor shall keep the Employer informed in advance of the time of starting of the progress of manufacture of material in its various stages so that arrangements can be made for inspection. Record of routine test reports shall be maintained by the Contractor at his works for periodic inspection by the Employer's representative. Certificates of manufacturing tests shall be maintained by the Contractor and produced for verification as and when desired by the Employer. No material shall be dispatched from its point of manufacture until it has been satisfactorily inspectedand tested.

Testing shall always be carried out while the inspection may be waived off by the Employer in writing only. However, such inspection by the Employer's representative(s) shall not relieve theContractor from the responsibility for furnishing material, software, and equipmentto conform to the requirements of the Contract; nor invalidate any claim which the Employer may make because of defective or unsatisfactory material, software or equipment.

3.7.4 Inspection and Test

All materials furnished and all work performed under this Specification shall be inspected and tested. Deliverables shall not be shipped until all required inspections and tests have been completed, all deficiencies have been corrected to Employer satisfaction, and the equipment has been approved for shipment by Employer. Should any inspections or tests indicate that specific hardware, software or documentation does not meet the Specification requirements, the appropriate items shall be replaced, upgraded, or added by the Contractor as necessary to correct the noted deficiencies.

After correction of a deficiency, all necessary retests shall be performed to verify the effective-ness of the corrective action. The test shall be considered complete when (a) when all variances have been resolved, (b) all the test records have been submitted and (c) Employer acknowledges in writing the successful completion of the test.

3.7.4.1 Inspection

Access to the Contractor's facilities while manufacturing and testing are taking place, and to any facility where hardware/software is being produced for Employer shall be available to Employer representatives. The Contractor shall provide to Employer representatives sufficient facilities, equipment, and documentation necessary to complete all inspections and to verify that the equipment is being fabricated and maintained in accordance with the Specification.

Inspection rights shall apply to the Contractor's facilities and to subcontractor facilities whereequipment is being manufactured. Inspections will be performed by Employer, which will include visual examination of hardware, enclosure cable dressings, and equipment and cable labeling. Contractor documentation will also be examined to verify that it adequately identifies and describes all wiring, hardware and spare parts. Access to inspect theContractor's hardware quality assurance standards, procedures, and records that are applicable to the facilities shall be provided to Employer.

3.7.4.2 Test Plans & Procedures

Test plans for both factory and field tests shall be provided by the Contractor to ensure that each test is comprehensive and verifies all the features of the equipment are tested. The test plans for factory and field tests shall be submitted for Employer approval before the start of testing. The contractor shall prepare detail testing procedure in line to specification and submit for Employer's approval. The procedure shall be modular to the extent possible, which shall facilitate the completion of the testing in the least possible time.

3.7.4.3 Test Records

The complete record of all factory and field acceptance tests results shall be maintained by the Contractor. The records shall be maintained in a logical form and shall contain all the relevant information. The test reports shall be signed by the testing engineer and the engineer witnessing the tests.

3.7.4.4 Reporting of variances

A variance report shall be prepared by either Employer or Contractor personnel each time a deviation from specification requirements is detected during inspection or testing. All such variances shall be closed in mutually agreed manner. However, at any stage if Employer feels that quality of variances calls for suspension of the testing the testing shall be halted till satisfactory resolution of variances, which may involve retesting also.

3.7.5 Factory Test

The factory tests shall be conducted on all the equipment and shall include, but not be limited to the following, appropriate to the equipment being tested:

- Verification of all functional characteristics and requirements specified.
- Inspection and verification of all construction, wiring, labeling, documentation and completeness of the hardware Before the start of factory testing, the Contractor shall verify that all changes applicable to the equipment have been implemented. As a part of the factory tests, unstructured testing shall be performed to allow Employer representatives to verify proper operation of the equipment under conditions not specifically tested in the above structured performance test.

The Contractor's test representative shall be present and the Contractor's technical staff members shall be available for consultation with Employer personnel during unstructured test periods. All special test facilities used during the structured performance test shall be made available for Employer's use during unstructured testing.

Factory acceptance Test (FAT) methodology - This shall be as per Section-7.7 in Part-B of this technical specifications. And FAT methodology for other auxiliary equipment such as APS, DG Set, VC equipment etc., have been specified in the relevant sections of this specification.

3.7.6 Field Performance Test

After the equipment has been installed, the Contractor shall start up and check the performance of the equipment of field locations. All hardware shall be aligned and adjusted, interfaces to all inputs and outputs installed, operation verified, and all test readings recorded in accordance with the Contractor's recommended procedures.

The field performance test shall exhibit generally all functions of the equipment and duplicate factory test. All variances must be corrected prior to the start of the field performance test. The list of final tests to be carried out in the field shall be listed in the site-testing document.

3.7.7 Type Testing

Type Tests shall be defined as those tests which are to be carried out to prove the design, process of manufacture and general conformity of the materials to this Specification. Type Testing shall comply with the following:

a) The Contractor shall submit, within 30 days of Contract Award, copies of test reports and certificates for all of the Type Tests that are specified in the specifications and that have previously been performed. The type test reports submitted shall be of the tests conducted within last five (5) years prior to the date of bid opening.

   In case the test reports are older than five (5) years ago on the date of bid opening or the type test reports are not meeting the specification requirement, the contractor shall carry out the type testing at no additional cost to the Employer/Owner.

   These certificates may be accepted by the Employer/Owner only if they apply to materials and equipment that are essentially identical to those due to be delivered under the Contract and only if test procedures and parameter values are identical to those specified in this specifications carried out at nationally/Internationally accredited labs and witnessed by third party / customer's representatives.

b) Type Tests shall be performed for all equipment types for which certification is not provided as required in (a) above, or if it is determined by the Employer that the certification provided is not acceptable. If any of the type tests are required to be carried out, the same shall be carried out by the Contractor **at its own cost.**

c) Type Tests shall be certified or performed by nationally/internationally reputed laboratories using material and equipment data sheets and test procedures that have been approved by the Employer. The test procedures shall be formatted as in the specifications and shall include a complete list of the applicable reference standards and submitted for Employer approval at least four (4) weeks before commencement of test(s). The Contractor shall provide the Employer at least 30 days written notice of the planned commencement of each type test.

d) The Contractor shall provide a detailed schedule for performing all specified type tests. These tests shall be performed in the presence of a representative of the Employer/Owner.

e) The Contractor shall ensure that all type tests can be completed within the time schedule offered in his Technical Proposal.

f) In case of failure during any type test, the Supplier is either required to manufacture a fresh sample lot and repeat all type tests successfully or repeat that particular type tests at least three times successfully on the samples selected from the already manufactured lot at his own expenses. In case a fresh lot is manufactured for testing then the lot already manufactured shall be rejected.

g) **Type test (if it fail), the expenses for repeating the test and the expenditure of the Employer personnel for witnessing the Type Test shall be borne by the contractor**.

3.8 Documentation

The Contractor shall submit a comprehensive list of the documents as applicable for the offered system for Employer's approval immediately after signing of the contract and the documents shall be finalized as per the approved list. The schedule for submission/approval of documents shall be in line with the overall project schedule.

To ensure that the proposed systems conform to the specific provisions and general intent of the Specification, the Contractor shall submit documentation describing the systems to Employer for review and approval. Further the Contractor shall also submit the drawings/documents for all the hardware &software required for site installation, testing and commissioning and thereafter operation of the system.

The Contractor shall obtain approval of Employer for the relevant document at each stage before proceeding for purchase, manufacturing,system development, factory testing, erection, site testing, training etc. Each document shall be identified by a Contractor document number, the Employer document number, and the Employer purchase order number. Where adocument is revised for any reason, each revision shall be indicated by a number,date, and description in a revision block along with an indication of official approvalby the Contractor's project manager. Each revision of a document shall highlight all changes made since the previous revision.

The Contractor shall submit two hard copies of each document/drawing for Employer's review and approval along with soft copy with each submission. After approval two set of all the documents shall be submitted as final documentation, however, for site specific documents two sets of documents shall be provided for each site. Any changes observed during field implementation shall be incorporatedin the as-build drawing and required sets of same shall be submitted to Employer.

In addition to hard copies all documentation shall be provided in electronic form preferably in pdf format. These documents shall be editable, searchable and printable. For this a web based "**Document Management System" (DMS)** software shall be supplied and installed at the owner's facility by the contractor along with minimum **50** number of client access licenses. DMS shall have multiuser capability with user role and privileged management. DMS shall have complete capability of tracking the documents version, ownership and editing. This DMS shall be used as central document repository for the entire lifecycle of the Project for easy managing and referencing of the project documentation.

This Document Management System shall have a facility to integrate the Owner's made documentation for system Operation to be used by Operator. The technical specification of the DMS is described at clause 4.8.4, Section 4, Part B, Vol II of this specification. In case any documentation requirement is specified in the relevant section the same shall apply for the equipment/ system defined in that section. The following document shall be submitted as applicable for the subsystem.

- Document identification plan
- System Description Documents (Overview)
- Functional Description Document (FDS)/Functional Cross Reference Document
- Data Requirement sheets
- Software Design Document
- Data base Documents
- Drawings/Documents for manufacturing/Assembly of the equipment/ system
- Drawings/Documents for installation of the equipment/system at site
- Software description/design documents for each module
- Factory Test report
- Manuals for each equipment
- System Configuration Parameter Details and procedure for configuration of all supplied equipment
- Site Testing documents
- Training documents
- System Administrator Documents
- User guide for Dispatcher
- Software Licenses
- Type test reports
- Battery sizing calculations
- Cable sizing calculations
- Inventory of the hardware
- Panel General and Internal Arrangement drawing indicating modules, components location etc.
- Installation drawing.
- Schematic drawing.
- External cable laying & termination schedule details (aa)
- Communication Channel Plan
- Firewall and security setup check list
- Configuration of firewall, routers, (ports allowed as per application

requirements).

The Contractor shall also supply two sets of User manuals/guides, O&M manualsand manufacturer's catalogues for all the hardware & software supplied under the contract one set each of which shall be at all the locations where the System has been installed. The user manual shall at minimum include the principle of operation, block diagrams, troubleshooting and diagnostic and maintenance procedures.

Considering all the components of the project briefly the following documents/drawings shall be required under the project. It is not acceptable to supply user manuals of systems, functions and applications as it exists. The user manuals shall be oriented towards system users and system deployed. All configuration and document entry related to project in DMS as per customer's requirement shall be the responsibility of the contractor.

The documentation pertaining to third party or OEM products may be supplied in the format as available from the third party/OEM. If both formats (Paper/electronic) are available then the above mentioned copies of documents shall be supplied in both the formats, however, in exceptional cases where the Contractor is not able to get more copies due to copyright laws restriction, the issue will be mutually agreed upon on case to case basis. The documents to be submitted shall include the following information.

3.8.1 Software Inventory

An inventory of all software shall be maintained by the Contractor. The Contractor shall submit the following inventory lists: the preliminary inventory list at the time of the FDS approval, an updated inventory list immediately prior to the start of the FAT, and the final inventory list at the time of system commissioning.

The inventory shall include the name of each program, a cross reference to pertinent Contractor documents, language and libraries used, and an indication of whether the programis to be standard, modified, or custom.

3.8.2 Functional Description

Functional description documentation shall be provided for each function described in Part B and shall cover how the proposed solution shall meet the required functionality as per technical specification. It shall include the following information for each function:

- Introduction describing the purpose of the function with references to otherdocumentation to aid the reader's understanding of the functions performed.
- Performance requirements that describe the execution periodicity and the tuning parameters that control or limit the capabilities of the software.

- Complete description of the operation, data and logic interfaces with other functions.
- Sample displays where applicable.
- Functional document which shall cover how the proposed solution shall meet the required functionality as per technical specification.

3.8.3 Software Design

Software design documentation shall be provided for each function, at least three months before the Factory Acceptance Test. It shall include detailed descriptions of the following items:

- The overall organization and structure of the software logic such as a breakout of the software into software modules.
- Complete description of the algorithms, operation and the data and logic interfaces with other functions.
- Interfaces with other software modules.
- Design limitations such as field length and the maximum quantity of data items that can be processed.

3.8.4 Database Documentation

Database documentation shall describe the structure of the database. The documentation shall define the individual elements (files, records, fields, and tables) and their interrelationships for Historian database also. Portions of the database developed specifically for Owner's systems shall be identified.

Documentation shall also be provided that instructs the user in the preparation of data to be used for the databases, including:

- The overall organization of input records.
- The format of each data record.
- Each data field and the valid entries pertaining to the fields.
- Frequency of Storage.
- Sampling of data for update in SCADA and storage in historian.

Sufficient database documentation shall be provided to enable the database to be updated or regenerated when inputs are changed and added, programs are modified, and new programs are added. Database access documentation shall be supplied such that software developed by /Owner may use the same access tools used by the Contractor-supplied software.

3.8.5 User Documentation for Dispatchers

User documentation for dispatchers shall contain detailed operating instructions and procedures. Information in the documentation shall be presented in terms that are meaningful to dispatchers. Each system function of this Specification and all other functions designed for dispatcher use shall be included in this documentation. Instructions and procedures shall be explained step-by-step with an explanation of how each step is performed, which parameters can be adjusted, and the effects obtained by varying each parameter. Additionally, the user documentation shall describe:

- All user guidance and error messages, along with the steps necessary to recover from errors.
- The user interface including displays and keyboard operations used to control and review input to and output produced by the function. All displays relevant to the function shall be included along with a description of each dynamic display field.
- Alarms and messages issued by the function and the conditions under which they are generated.
- Procedures to be followed as a result of computer system restarts, failures, and failovers.
- Initially both Main & backup control Centre shall operate active-active mode and their various combination of operation in case of failures in communication/control center.
- Main & backup control Centre Switch Over Dispatcher documentation shall be customized separately for Owner's system of main and Backup and shall be based on the delivered systems. It is not acceptable to describe the Contractor's standard system and then identify differences between the standard and delivered systems. The documentation shall not include standard or other descriptions that do not apply to the delivered systems.

3.8.6 System Administration Documentation

System administration documentation shall be provided to guide owner's personnel in the operation and procedures required to generate and update the systems, including system software, database, application software, and other elements of the systems. System administration documents shall be provided for the following items:

- Software management
- Network communications management
- Processor configuration
- System performance monitoring

- System restart/failover management and diagnostic procedures
- System generation and management
- Database generation and management
- Display generation and management
- Report generation and management
- Diagnostic programs
- Software utilities
- Software maintenance
- Application software parameters and tuning guides
- Any Other Contractor-supplied system software not included above.
- Switch Over from Main to backup
- Cyber security related documents i.e., Firewall policy, Access control, Device configuration, System hardening etc.

3.8.7 Test Documentation

Documentation for all factory, field, and availability tests that apply to Owner's system shall be provided in accordance with the requirements defined in **Section7 of Part-B**.

3.8.8 Training Documentation

Training documentation shall be provided for all courses in accordance with the requirements defined in the specifications **Section 2 of Part A**.

The Contractor shall submit a comprehensive list of the document as applicable for the offered system for Employer's approval immediately after signing of the contract and the documents shall be finalized as per the approved list. The schedule for submission/approval of documents shall be in line with the overall project schedule.

3.8.9 Documentation of Auxiliary Power Supply System /DG SET

The following specific document for items covered under this section shall be submitted which shall be in addition to the applicable general document.

- Data Requirement Sheets (DRS)
- Cable sizing calculations
- Inventory of the hardware
- Panel General arrangement drawing
- Panel Internal General Arrangement drawing indicating modules, major devices/ components location etc.

- Installation drawings
- Schematic drawings
- Type Test reports
- FAT plan & procedure
- SAT plan & procedure
- External cable laying & termination schedule details
- Availability test plan & procedure

3.8.10 Documentation of Video conferencing System

The following specific document for items covered under this section shall be submitted which shall be in addition to the applicable general document.

- Hardware description document
- Testing plan & procedure
- Layout, installation, GA, BOQ, schematics and internal wiring drawings for each site
- Availability test plan & procedure
- Operation & Maintenance document
- Training documentation

3.8.11 RTU/Terminal Server/DCPC Documentation

The Contractor shall submit sets of all the standard and customized RTU documents for review and approval which includes the following:

- RTU/Terminal Server/DCPC Function design document
- RTU/Terminal Server/DCPC Hardware description document
- RTU/Terminal Server/DCPC Test equipment user documents
- RTU/Terminal Server/DCPC Operation & Maintenance document
- RTU/Terminal Server /DCPC Training documentation
- RTU/Terminal Server/DCPC Database document
- RTU/Terminal Server/DCPC Test procedures
- Data Requirement Sheet (DRS) of all items
- RTU/Terminal Server/DCPC installation and Layout, GA, BOQ, schematics and internal wiring drawings for each RTU site
- RTU/Terminal Server/DCPC to C&R panels/ field device cabling details

for eachRTU/Terminal Server /DCPC site After approval of all the above documents, the Contractor shall submit two sets asfinal documents.

The site-specific drawings as indicated as above shall be submitted in two sets for each site before installation of RTU/Terminal Server/DCPC. In case some modifications/corrections are carried out at site, the contractor shall submit the same as built site-specific drawings in two sets after incorporating all suchcorrections as noticed during commissioning of the RTU/Terminal Server/DCPC.

---**End of Section 3----**

Section 4

Maintenance & Support Services

Table of Contents

Section 4 Maintenance & Support Services

4.1 Introduction

The scope of work under maintenance & support services shall include a comprehensive maintenance of all the software & hardware (All equipment, peripherals, cables, panels etc.) supplied by the contractor for the complete systems viz SCADA/EMS, Video Projection System, RTUs, Video conferencing system, Auxiliary Power Supply system, DG set & Cyber security system etc. along with the future integration and support services for meeting the future requirement envisaged under this project. The maintenance practices to be followed shall be as per ISO 20000 Standard. The essence of the maintenance and support services is to provide maintenance support for the entire system (hardware and software) supplied by the Contractor, with the goal of meeting the availability as set forth herein.

The availability of all the equipment/items supplied under the contract is the essence of the contract. Contractor shall maintain required availability of the system during entire period of the contract as per the terms and conditions and requirements mentioned in document. The maintenance of all the supplied system comprises of all activities required to keep the systems up and running all the time at an optimum level by proactive monitoring, diagnosis and rectification of any failure of all the hardware(s) and software(s). The 24x7x365 support shall be provided by Contractor.

4.2 Maintenance support

The period of maintenance support shall consist of one-year Warranty (Defect Liability) period (Defect Liability period extendable, if defects found) commencing from Operational Acceptance and six years Maintenance period thereafter. **Payment will not be released during defect liability period**. The Owner at their own discretion may extend the duration of maintenance period for up to 2 years based on the same rates, same terms and conditions of the contract. For any addition (e.g. integration of new RTUs or new control center) during maintenance period, contractor shall provide all the services **at control center end** without any additional cost **during entire period of the contract including extension (if any).**

The nature of maintenance support required for different type of systems and components are described in the Table 4.1 below:

Table 4.1 Maintenance support and Availability requirements

System	Scope	System Availability requirements
All systems & subsystem such as SCADA, EMS, AGC, ICCP, Web System, Historian, NMS, VPS, Video Conferencing System, Cyber security system etc. supplied in this project	Hardware and software in Control centres	99.99%
APS, DG set		99.99%

The system availability shall be measured Control Centre wise, for example the availability of Main Control Centre and Backup Control Centre shall be considered separately. Similarly, the availability of various systems for e.g., SCADA/EMS System (Hardware and Software & Video Projection System) shall be considered separately at each of the control Centers.

For all third-party equipment (Hardware & Software) Contractor shall have back-to-back support & warranty along with supply of spare with appropriate response time from OEM and these Back-to-Back contracts will be shared with owner before start of defect liability period. The contractor shall be responsible for coordination with the OEM for all matter related to that equipment.

The Contractor shall be responsible for meeting the overall response times and availability requirements specified in the Specification. Contractor shall also be responsible for hardware/software replacement/upgradation without any additional cost in case OEM declares end of life/end of support/ obsolescence for the product.

The maintenance of the System shall be comprehensive and shall comprise of the following category of works which is further elaborated for each of the different subsystems:

(a) Preventive Maintenance Activity (performance monitoring, system backup, patch management, updates, emergency response and troubleshooting)

(b) Maintaining a minimum no. of specified spares on a continuous basis.

(c) Integration of new equipment (RTU/Terminal Server, Workstations, Printers, Switch, Router etc.) and integration of a new or existing Control Centre on ICCP with the Main & Backup Control Centre Systems or any other control centre.

(d) In case field device supports Secure IEC 60870-5-104 protocol, same shall be integrated in secure mode at control centre end.

(e) Database and Display development (including all ICCP & ADMS/LSS configuration) during the AMC period shall be under the scope of the contractor. To meet the requirement, if the placement of any additional manpower will be required same may be provided without any additional cost to the Owner.

(f) OEM Back-to-back Support:

i. All the supplied system shall be under OEM (Hardware and Software) warranty & support till the completion of entire AMC period (including extension of contract, if any).

ii. During entire contract period (including extension of contract, if any), if OEM discontinues/ declared ends support to any item supplied (software/hardware/security solution/OS) under the contract, contractor has to replace such hardware, software (or both, depending on software or hardware dependencies on each-other) without any additional cost to Owner. Replacement shall be of either the same or higher configuration keeping required performance specified under the contract and it shall be from the same OEMs. OEM can be changed only after the receipt of letter from OEM regarding non-availability of **similar or higher configuration** of non-supported item(s).

iii. If any development, customizations, testing, etc. needs to be done for the compatibility of SCADA/EMS and other applications on the new OS platform, Anti-virus and any other software delivered in the project upgradation, then the same shall be done by the contractor at its own cost.

iv. Contractor has to submit annually documentary evidence for the availability of OEM supports for the supplied items including continuity of security patches.

v. Quarterly payment shall be released after the submission of valid OEM support for all the supplied system.

(g) Owner shall be able to login independently to OEMs (hardware and Software) portal (if available) to view support contracts and raise TAC/ RMA directly with OEM if required.

(h) Owner shall be able to use a self-web log-in to register a complain through SCADA OEM web portal. Portal shall have auto escalation provisions after a lapse of pre-defined time.

i. Signature updation though out the contract period including AMC of various software licenses supplied under this project shall be in scope of the contractor.

ii. Contractor has to submit proper cyber risk mitigation plan/risk offered by connecting the system to the internet (whenever required) along with necessary cyber security measures in place. The contractor is allowed then only when the plan is approved by the owner.

iii. Contractor shall provide support during mock drill of main and backup control center failover process which shall be performed periodically as per respective owners.

iv. C10 Capacity test shall be done periodically (yearly), to determine whether the rating of battery is holding up using capacity test. If the battery capacity is less than 80% of its design value in any of the cases, the battery shall have to be replaced by contractor during entire period of contract (including extension of contract, if any) without any cost implications to owner. If number of cells replaced(cumulative) in battery bank exceeds more than 25% of total battery bank in any of the cases during entire period of contract (including extension of contract, if any), then contractor shall replace that entire battery bank without any additional cost to the Owner. Also, Refer Section 3 & Section 8 PART C of TS.

v. The contractor shall submit the undertaking format as per format mentioned at Appendix-K of Part-A for new items as well as repaired items supplied under this project.

4.3 Preventive Maintenance Activity

The preventive maintenance activity comprises of the activities to be performed by the Contractor to keep the system running at optimum level by diagnosis and rectification of all hardware and software failures and would broadly include.

(a) Repair / replacement of defective equipment. The Contractor shall be responsible for repair/replacement of all the hardware including consumables required for various systems. Only replacement of printer cartridge and paper rim shall be excluded from the scope of the Contractor.

(b) Configuration of the replaced hardware and software, periodic routine checking as part of a preventive maintenance program (as described in further detail in this document) which would include checking of functionality of hardware and software.

(c) Monitoring of the performance of the system and doing necessary tuning for optimum performance to accommodate any changes such as the addition of new components.

(d) Providing all necessary assistance to Owner as per Responsibility matrix defined in this section.

(e) Auto Backup of the system at regular interval and Monitoring of all auto backup scheduled.

(f) Addition and modification of database and displays, report generation and Database sizing activities etc. and other day-to-day operational activities would primarily be the responsibility of Contractor.

(g) Database sizing activities including Backup and restore of the system. Any replacement or upgrade of hardware and/or software to meet the power system sizing as per table in Appendix would be the responsibility of the contractor at its own cost.

(h) Restoration of the systems upon its failure and to restore the functioning of the various systems at the respective Control Centres.

(i) Detailed scope of work during warranty & AMC are mentioned under clause 4.9.

(j) Verification of endpoint security updates

(k) The contractor shall maintain register for all the activities carried out during preventive maintenance.

(l) The contractor shall maintain list of inventories of all hardware and software items being supplied along with software bill of material (SBoM). The inventory shall include version/firmware number for understanding of applicable vulnerabilities from publicly disclose vulnerabilities databases and shall take required action.

(m) Taking an Image back-up of all the Systems. At any time, Last four (04) image back-up shall be maintained. Back-up image shall be tested once in three (03) months using spare servers of all systems. Two (02) copies of back-up shall be maintained on backup appliance (along with other backup details mentioned in Appendix-H, PART-B) and another Two (02) copies shall be maintained, out of which one shall remain with Contractor on SAN/NAS and other with Owner. Contractor shall provide the hard disks (as per item mentioned in BoQ.) for the back-up for owner's copy. If no BoQ item is mentioned for HDD then Owner shall provide the hard disks for the back-up of owner's copy.

(n) Routine works like database building, addition of analog and status points, report generation etc. and other such day-to-day operational activity would primarily be the responsibility of Contractor and the same shall be completed in close coordination with Owner.

4.3.1 Hours of Cover

The Contractor shall provide engineers who have an experience and skill to maintain the SCADA/EMS system (including Cyber Security measures) to the desired level of availability. The contractor's on-site support for Main Control Centre and Backup control Center shall be standard hours of service i.e. Monday to Saturday- 9:00 am to

5:30 pm local time (IST), excluding public and Owner Company holidays, throughout a year. Hardware, Software and Network engineers (wherever applicable) having expertise in SCADA/EMS system shall be deployed at respective control centres during the standard hours of service as per below mentioned table: (The Software Engineer to be deployed during AMC shall have experience in Cyber Security also along with the SCADA/EMS system).

Sl. No.	**Control Centre**	**Number of manpower at control centre**			**Remarks**
		Main	**Back up**	**Sub-LDC**	
1	For ERLDC	3 (1 H/W, 1 S/W, 1 N/W)	2 (1 H/W, 1 S/W)	-	Hardware (H/W), Software (S/W), Network (N/W) (wherever applicable)
2	For each SLDC	2 1 H/W, 1 S/W)	1 (1 S/W)	-	

Manpower requirement for RTUs AMC:

S.No.	**Name of SLDC**	**No of Manpower required during AMC**	**Remarks**
5	Sikkim	**2 (Two)**	1 RTU Engineer for Main SLDC & 1 RTU Engineer for backup SLDC
6	JUSNL	**2 (Two)**	

Note: ***The above manpower requirement during AMC period is indicative only, in case of critical defects in the system, if any, additional manpower shall also be deputed by the Contractor at no additional to Owner and up to the satisfactory closure of the critical issues during the tenure of AMC.***

There shall be provision for rearrangement of engineers between the control centres (main, backup, sub-LDCs) as per owner requirement during entire contract period

The timings for Emergency Support would be 24 hours a day, 7 days a week throughout the year. Total working day envisaged is six per week, Owner at his discretion can use any day/time of the week (including weekends i.e., Saturday or Sunday) considering the work requirements and timing shall be as per Owner requirement.

The support personnel so deployed shall be qualified personnel having at least 2 years of experience in the SCADA/EMS system including one-year experience in the delivered SCADA/EMS system. The person deputed shall be a permanent employee on the direct pay roll of the contractor. The contractor shall submit the CV's of the persons to be deputed to Owner for approval before their deploymentat site. The Owner can ask the Contractor to replace the personnel deployed for maintenance support if his performance is not found to be satisfactory.

The Contractor is required to organize a team located in India composed of specialized and experienced staff (his or the system's manufacturer), responsible for the technical support of all System applications. The Contractor shall disclose the names, addresses, e-mails, telephone and fax numbers along with Escalation Matrix as well as any other information necessary for the RLDC/SLDC's to communicate with the staff, as well as each person's scope of responsibility within the framework of this Contract. Additional Contractors "helpdesk"/call centre information shall be submitted to the RLDC/SLDC's along with the procedures and respective time response.

The onsite support staff should possess capability for supporting the equipment and components proposed, but not limited to undertaking preventive and break-fix maintenance, troubleshooting, resolving problems, tuning etc. The Contractor shall also provision for necessary offsite support to ensure continuity of operations.

The Contractor within the frame of this contract is required to provide information for modification and improvements for the system. Contractor shall provide access to technical support and contractor's technical database, by providing the RLDC/SLDC's responsible staff with the relevant username and password, for the purpose of submitting technical questions and problems.

Contractor and its personnel have to follow all rules and deregulations of Owner office premises in view of Owner certifications of ISO-9001, ISO-14001, OHSAS-18001 and ISO- 27001 including any other future certification.

4.3.2 Service Response requirements

The severity levels are defined in coming sections and the requirement of response time for various severity levels is defined below:

Emergency Support for Severity 1 issues are to be provided **24 hours a day, seven days a week**. The on-call support team shall include all key technical competencies so that any aspect of a system failure can be attended. The team shall comprise of experienced technical staff that are skilled in troubleshooting of the various systems covered under AMC. Severity 1 problems shall be reported by telephone or any other communication media for rapid response; target response times are defined in para 4.6 of this section.

For severity 1 problems, the key objective is to restore the system to an operational state as quickly as possible, including by a temporary workaround. Resolution of the defect may be completed during standard hours. Severity 2, 3, and 4 problems shall be reported by Owner through a call tracking system to be provided by the contractor. Resolution of problems may also be provided by an individual fix that will be installed by the contractor at no extra cost to Owner. Resolution of problems shall be completed within the specified response & resolution time mentioned in this specification.

4.3.3 Monitoring

The operation and performance of the various systems under AMC shall be monitored on a fortnightly basis, the contractor shall review the following, analyze the results, and submit report to Owner. **Non-compliance to Monitoring of Log, Patch Management, Bi-Annual Security audit and implementation of the remedial actions suggested by the auditor will be treated as Severity 2**. The contractor shall conduct at least the following monitoring, for the all-Control Centres.

4.3.3.1 Log Monitoring

(a) System logs for a selected day

(b) System history log

(c) Aggregate data collection

(d) Events Collection

(e) Configuration change to core application/OS.

Log monitoring and report generation for non-availability period of ICCP links and other communication links shall be done. Compiled report shall be generated based on the requirements.

During monitoring if any defect/ abnormality is found, the contractor shall undertake corrective maintenance for the same. The contractor shall submit the process details to meet the above requirements.

4.3.3.2 Resource Monitoring

Resource Monitoring services comprises checking the system's major node resources,gather log data, analyze results, and advise Owner on the appropriate actions to be taken and undertake any agreed upon actions. The NMS system shall be used to continuously collect the following information: -

(a) CPU loading (Peak and Average)

(b) Memory utilization (Peak and Average)

(c) Disk utilization (Peak and Average)

(d) LAN utilization (Peak and Average)

(e) Operating system resource utilization reports

(f) System error log

(g) Average disk transfer per second

(h) Temperature

The Contractor shall submit the procedures details to meet the above along with the offer.

4.3.3.3 Cyber security System monitoring and Monitoring and compliance manager for Critical Infrastructure Protection

The Contractor shall also be responsible for monitoring of the cyber security system with cyber security perspective and implementing the monitoring and compliance manager for Critical Infrastructure Protection. The logs of the system shall be analyzed for exceptions and the possible incident of intrusion/trespass shall be informed to the Owner promptly.

The monitoring shall encompass the various cyber security devices installed at Control Centre such as firewalls, Intrusion prevention system (both network based and host based), routers etc. All advisories given by CERT-In / CERT-GO/NCIIPC /CEA/ **Meity** etc. shall be complied with in the timely manner **during entire contract period including extension of contract, if any.**

The Cyber security system shall also be subjected to six monthly Security Audit/Configuration audit from CERT-In listed auditors at the cost of the Contractor.

The contractor shall adapt all relevant advisories issued from time to time by any statutory authority in timely and effective manner throughout the period of contract.

The contractor shall carry out the six monthly (bi-annual) Cyber Security Audit including vulnerability assessment and penetration testing from CERT-In certified auditors at its own cost for the complete systems under this project during entire AMC period and implement the recommendation given by auditor in consultation with the Owner. **Each auditor along with auditing firm need to be mandatorily changed after 3 consecutive audits so that different auditors audit the system throughout the maintenance phase including extension if any.**

Experience of cyber security auditing firm– The cyber security auditing firm must have carried out audit of at least one number of critical infrastructure site identified by NCIIPC during last one year.

SOP issued by NCIIPC for auditing of CIIs/Protected systems by Private/Government Organisation shall be followed by the contractor during cyber security audit along with its amendment/revision.

The contractor shall ensure confidentiality and submit the NDA from cyber security auditor firms before auditing to the owner. The format shall be provided by owner.

Every Bi-Annual Cyber Security Audit shall be conducted in phase-1 and phase-2, phase-1 initial audit (as per periodicity) and Phase-2 is follow up audit of phase-1 to check the closing of phase-1 audit observations. Contractor shall implement the recommendations/remedial actions suggested by the Auditor after the initial audit for any upgrade (Patches) in existing system **within 1 month** of phase-I cyber security audit. The same shall be verified in Phase-2 audit within 1 month of the phase-1 audit. The Contractor shall submit signed reports for phase-1 and phase-2 audits (signed by Certified Audit agency) to the Owner.

In case VAPT/cyber audit during AMC period suggest deployment of any new hardware/software solution to further improve cyber security posture, which was not envisaged under this supply/services contract then the same shall not be considered under contractor's scope.

Cyber audit shall be deemed successful and complete when verification for vulnerabilities of previous audit is compiled duly signed by auditor within time stipulated as per statutory guidelines. Detailed scope of work for Cyber Security Audit is given in **Part-A, Appendix-G.**

There shall not be any separate charges for service/integration of the Hardware/Software as per the recommendation of "Cyber Security Auditor".

Any vulnerability reported by the owner shall be addressed by the contractor.

4.3.4 Patch Management

The contractor shall also be responsible for providing updates/patches for the software products supplied under the project and acquisition of security certificate (including list of Certificates which have been revoked, expired, hold) from Certificate Authority for implementation of secure ICCP**.** All other patches of third-party products like Operating System and Anti-virus shall be tested by the Contractor prior to installing in the Owners network. Other products like IPS, Network IPS, and Host based IPS, Firewalls shall also be provided with secure patch management. A secure patch management and deployment system is to be established which shall be provided with single point of Internet connectivity. All the patches shall be downloaded through this single point of connection. **The patch management of SUBSLDC and remote consoles supplied under the project shall be done by the contractor through respective SLDCs/RLDC**.

The Contractor shall provide a mechanism for patch management so that it is known which patches have been applied, which patches are pending but available with system and what is the recent release of patches for the various products. Any patch shall be applied only with express permission of the Owner's representative.

The contractor shall ensure that all systems are maintained with latest patches/releases implemented. Patches/signature/firmware/updates (wherever applicable) shall be completed as per given timelines, if contractor fails to comply the timelines given below, it will be treated under severity clause as given in Para 4.5.

The contractor shall upgrade the various applications delivered under the project through patch management and version upgrade to make it compliant with IEC standards as envisaged under the specification **during entire contract period including extension of contract, if any**. Updated patches shall be applied in the system within the timelines given below. Non-compliance will be considered under severity-2.

Sl. No.	Devices	Time Lines from the date of Release
1.	Server	2 months

Sl. No.	Devices	Time Lines from the date of Release
2.	Work Stations	1 week
3.	Anti-virus / Firewall/HIPS /HIDS/Network IPS signatures	Daily
4.	Server/Workstation/Network Devices/Firewall Firmware upgrade	1 month

4.3.5 Physical maintenance

The contractor shall undertake physical maintenance of all equipment/modules under the scope of this contract, in accordance with this section. The physical maintenance shall include cleaning, dusting, inspection, tagging/retagging of equipment for loose connections, damage to insulation pest infections, damage due to rodents etc. followed by submission of quarterly report:

Activities shall include, but not be limited to: -

(a) Online diagnostics for servers and workstations – once every 3 months.

(b) Connection test of LAN cables for identifying potential loose contacts in machines, switches and routers - once every 3 months.

(c) Physical hardware checks to ensure proper working of cooling fans etc. - Once every 3 months.

(d) Physical inspection to check the machines and the panels for rat droppings, lizards or other vermin - once every 3 months.

(e) Cleaning and blowing for removal of dust from servers, Workstations and CFE panels etc. of supplied system - once every 3 months. The preventive maintenance would include checking and diagnostic functions for software also.

<u>Exclusions: -</u>

(a) Interfacing panels cleaning etc. are excluded from the scope above.

(b) Maintaining dust free environment and protection from rodents and vermin is the responsibility of Owner.

(c) Regular cleaning of computer furniture and surroundings is the responsibility of owner. Planned & scheduled Equipment shutdown during preventive maintenance shall be deemed as available.

4.3.6 Video Projection System

The Video projection system shall have comprehensive maintenance contract with VPS OEM for the entire period of contract. Any consumables as well as any spares required for maintaining the VPS system in fully operational condition shall be provided by the contractor without any additional cost to Owner.

In addition to that there shall be quarterly checks from OEM of the video projection systems in whichthe brightness uniformity, brightness level, colour uniformity and other routine maintenance activities like cleaning, system tuning shall be UNDERTAKEN.

4.3.7 Preventive maintenance of Auxiliary Power Supply & DG SET

This consists of measures regarded as necessary to maintain the equipment in the proper operating condition. Preventive maintenance includes functional checking, cleaning and necessary repair, replacements, adjustments etc. It will be carried out quarterly at mutually agreed dates. The following checks need to be carried out: -

a) Physical inspection of UPS and its accessories
b) Cleaning of System
c) Tightening of all the power and control connections
d) Checking of output DC Voltage
e) Checking of AC Voltage L-L, L-N
f) Checking for batteries performance. Replacement of faulty batteries and or entire battery bank up to the completion of one year DLP and 6 years AMC period, (irrespective of the design/expected life of the supplied batteries) shall be in the scope of the contractor, without any cost implication to the Owner.
g) Checking for input AC current
h) Checking of output AC Current
i) Checking for any ripples
j) Checking for output frequency
k) Checking for transfer of UPS to Bypass and Bypass to UPS
l) Checking for UPS transfer to batteries after shifting the main load on other UPS

& on dummy load equivalent to actual battery load.

m) Checking of UPS for Normal Operation

n) Checking of UPS PCB Parameters as per standard checklist of manufacturer.

o) Checking for cooling fans, other indication meters installed on the panel.

p) Checking earthing system by measuring earth to neutral potential.

q) Checking of present load on UPS

r) Matching of UPS parameters with monitoring system

Proper guidance to operation staff for satisfactory working of the equipment and its proper upkeep. Above observations shall be recorded as per Format A given in this section and duly signed by Owner.

4.3.8 Preventive and Break down maintenance of the supplied DCPS & Battery System

MAINTENANCE OF DC POWER SUPPLY SYSTEM

(DCPS includes charger, Batteries, DCDB and other associated cables/connectors, Meters, relays, switches, surge protection devices etc.)

The Contractor shall carry out both preventive and breakdown maintenance of the supplied DCPS & Battery System.

Preventive Maintenance (PM)

This consists of necessary measures to maintain the equipment in the proper operating condition. Preventive maintenance includes functional checking, cleaning and necessary repair/replacement/adjustments etc. It will be carried out quarterly at mutually agreed dates.

Break Down Maintenance

Break Down Maintenance is to be carried out in the event of malfunctioning of DCPS equipment, which blocks the normal operation of the DCPS. Breakdown maintenance includes faultfinding, repair or replacement of defective parts and functional checking. Immediately on noticing the fault, the fault will be reported by the Owner on phone to the contractor. The fault reporting time on phone shall be taken as reference time for the purpose of RT and TAT.

(RT is Response Time when contractor's person report at site after reporting of fault in system. TAT is Turn-Around-Time when system is brought back in service after necessary rectification/replacement works.

A SCOPE OF WORK DURING MAINTENANCE PERIOD

MAINTENANCE OF DC POWER SUPPLY SYSTEM (DCPS includes charger, Batteries, DCDB and other associated cables/connectors, Meters, relays, switches, surge protection devices etc.)
Details of Job to be carried out during Preventive Maintenance **4.6.1.1** 1 Physical inspection of DCPS at all specified locations 2 Cleaning of System 3 Tightening of all the power and control connections including checking the input power cable terminations at both ends. 4 Checking of DC Voltage 5 Checking for AC Voltage L-L, L-N 6 Checking AC Current 7 Checking for ripple Voltage 8 Functional checking of DC System for Normal Operation including battery charging 9 Checking for Normal operation of each Module 10 Checking of earthing of the system by measurement of earth to neutral potential. 11 Checking of charging condition of the batteries 12 Checking of the physical conditions of the batteries 13 Checking of each battery voltage during quarterly visits & battery impedance/resistance measurement twice during the contract during 2nd & 4th quarterly visit. 14 Three discharge tests per year at normal load for three hours during 1st, 2nd and 4th quarterly visit.

15 Checking of present load on charger. 16 Matching of DCPS parameters with SCADA system 17 Proper guidance to the operation staff for satisfactory working of the equipment and its proper upkeep. 18 Checking of battery terminals for corrosion and cleaning thereof, torqueing and greasing. 19. C-3 discharge test on batteries once a year during 3rd quarterly visit. Above observations shall be recorded as per enclosed format and duly signed at site by Owner Engineer.
1. Repair and replacement of Faulty Module
2. Repairing and replacement of faulty components in the system
3. Analysis report of the fault
4. Plan for preventive measure to arrest recurrence of such faults

4.3.9 Furniture

The Furniture and fixtures supplied with the system shall have comprehensive maintenance contract with OEM. Any spares required for maintaining the Furniture in fully operational condition shall be provided by the contractor **without any additional cost to owner.** In addition, there shall be quarterly checks of the Furniture for routine maintenance activities like repairing, working of motorized system etc.

4.4 Spares inventory

The Contractor shall provide/keep spare parts, hardware, software and all other materials, required for the preventive maintenance and repair of malfunctions occurring to the hardware and software covered by this contract, at his own expense and with no further financial charge to the Owner.

Minimum number of spares shall be kept at the respective Control Centers as mentioned in relevant section of technical specification shall be kept at the respective Control Centres, however, Contractor can maintain additional spares also to maintain the system as per the required availability of supplied system.
The spares shall be used as and when required and no separate charges are payable other than the **AMC** charges. All spare shall have pre-loaded software and all required licenses in order to make it readily available for use at all times. The Contractor shall be responsible for the availability and quality of these materials (tested and approved as regards reliability of operation).

The Contractor shall be responsible for keeping up to date records of the spare parts, hardware and all other materials available for the maintenance and shall notify the responsible RLDC/SLDC's office of all changes made as to the items and quantity of such items in stock.
Throughout the term of the Contract, the spare parts required to restore malfunctions occurring in critical system operations shall be allocated in such relevant RLDC/SLDC's locations. Every time a spare part is used, it shall be replaced immediately by another or it shall be repaired promptly so as to be ready for use again. This shall be periodically verified by the Owner and unavailability of spares shall be treated as non-availability as per severity 2 **if not replenished after a specified period**.

In case mandatory spares (**Table 4.2**) have been used in the system, the replenishment of such spare shall be done within 45 calendar days (for UPS Spares it shall be 15 calendar days), otherwise it will be considered as non-availability as per **Severity-2**. All Spares shall be fully loaded with licensed OS and all required Application Software etc. to test patch management and keeping ready to use during contingency and failures.

In case peripheral units or hardware units, covered by this contract, remain out of order for a period exceeding three (3) consecutive calendar days, or cumulatively per year for more than five (5) days, from the date of such malfunction or breakdown notification of the Contractor occurs more than three (3) times per month or six (6) times per annum, then the respective RLDC/SLDCs is entitled to demand immediate replacement of such units. Moreover, the Contractor is required to investigate the cause of such malfunction and to notify the respective RLDC/SLDCs as to the measures to be taken to avoid such similar malfunction from occurring in the future.

Further, in case Contractor failing to provide the replacement or fails to repair original equipment within defined period. Owner shall be at a liberty to get the system repaired/replaced through alternate source and debit/recover the cost including 15% overhead charges from the consolidated AMC charges payable. Owner shall entertain no correspondence or counter claim in this regard.

4.5 Integration of new equipment and or control centre

All future services, protocol emulations and configuration support for integration of RTUs, SAS, Control Centre integration on ICCP clients for OPC Services, Web services and CIM import and export utility for off-line applications shall be the responsibility of contractor during maintenance period. The integration services to be provided by the contractor will include the Communication Front End (CFE) configuration, addition of New ICCP connection and its integration, addition of interface for off-line Applications, OPC Clients etc.
Support at Control centre for these integration shall be treated as severity-3 support

as defined below.

For payment purposes, a separate BOQ item has been identified for such services and unit rate shall be used for payment purposes. If separate price not mentioned in BOQ, then it shall be considered as included in AMC charges and no additional charge will be paid.

The numbers specified in BOQ are indicative only. Actual number of RTUs and CCs integration during AMC period may vary. Payment to the contractor shall be based on the unit rate and actual number of RTUs or CCs integrated

4.6 Problem/Defect Reporting

The contractor shall submit an appropriate problem/defect reporting procedure to meet the requirement of all severity levels to get the approval of the same from Owner. The problems shall be categorized as follows:

Table 4-3 Severity Levels

Category	Definition
Severity 1 – Urgent	Complete system failure, severe system instability, loss or failure of any major subsystem or system component such as to cause a significant adverse impact to system availability, performance, or operational capability (as described at 4.5.1.1)
Severity 2 – Serious	Degradation of services or expiry of software licenses or critical functions such as to negatively impact system operation. Failure of any redundant system component such that the normal redundancy is lost (as described at 4.5.1.2) Non-availability of Man-power at Control Centre during working hours, non-availability of spares, cyber security compliance, patch Management, Non availability of Back-to-Back OEM warranty contract for third party hardware/software/solutions along-with its subscription.
Severity3 – Minor	Any other system defect, failure, or unexpected operation (as described at 4.5.1.3), patch application as recommended by Owner. Changes in configuration, or architecture carried out during AMC must be documented with clear document number.
Severity 4 - General /	Request for information, technical configuration assistance, "how to" guidance, and enhancement requests. (As described at 4.5.1.4).

Technical Help	

4.6.1 Severity levels

The detail of the systems under different severity levels is as below:

4.6.1.1 Severity-1 (Urgent support)

This support is required when there is a complete system failure, failure of both servers, severe system instability, the loss/ failure of any major sub-system / system or its components, which may significantly impact the system availability, performance, or operational capability at Control Centre.

Following outages/disruptions will be considered under **Serverity-1**:

a) Loss of Critical functionality as envisaged in specification due to any problem Software/Hardware-related in SCADA-EMS system, ICCP system.

b) Outages of **both** CFE system

c) Outage of both the redundant system (hardware, networking, software etc)

d) Cyber Security issues and outage of complete Web system

e) Outage of both Routers and LAN Switches

f) Outage of any Critical Functions as envisaged in Specifications

g) Outage of both main and standby routers, failure of both main and standby LAN

h) Outage of both main and backup servers of any system

i) Failure of main and standby firewalls

j) Loss of data exchange with other computer systems or other Control Centres would be included under this category.

k) Failure of complete UPS system resulting into loss of UPS output supply at both Output ACDBs is covered under this category if supplied under the project.

An SMS and Email alert shall be notified to the operators for outage of any critical services under Severity-1 of SCADA/EMS system.

Upon receiving intimation, the representative of the contractor would immediately attend to the problem. The problem shall be attended by the contractor at the earliest, and it shall arrange all resources and take all steps to restore the data availability and functionality at the earliest.

4.6.1.2 Severity-2

The support services not defined under Severity-1 are included under this category as mentioned below.

Coverage under this severity would be outages that do not immediately cause on line data loss but subsequently could result into Severity-1 category outage, loss of an important subsystem that may affect the day-to-day works and loss of archived data. Following outages/disruptions will be considered under Serverity-2:

a) Failure of one Data Server/ICCP server, stoppage of data collections for archiving & retrieval, failure in Acquisition of SOE at the respective Control Centre, and outage of other applications not covered under severity-1 are included in this category. However, the critical functionality loss due to loss of only one component as defined here shall be treated as Severity-1

b) Failure of one output ACDB, one input ACDB, failure of one UPS system, Failure of Battery System and failure of any other system of Auxiliary Power supply not covered under Severity-1 are included in this category. The **Failure of DG set when one of the UPS/battery bank is also failed simultaneously, shall be considered under Severity-1.**

c) Failure of any redundant system component affecting the critical redundancy like loss of any one Application Processor, Router and CFE would also be included in this category.

d) The failure of VPS. However, a maximum time of Organization and travelling of 48 hrs shall be provided in the worst case.

e) Outage of real-time data reporting, inability of user to create/edit display, database and calculations.

f) Cyber Security Compliance & Patch Management

g) Failure of one server/application of redundant system

h) Stoppage of data collections for archiving (provided data storing going on in pre-specified buffer).

i) Failure in Acquisition of SOE at the respective Control Centre.

j) Outage of other applications not covered under severity-1 are included in this category.

k) Non-availability of designated contractor's Man-power at Control Centre as well as replenishment of inventory of spares specified in TS will also be covered under this category. However maximum travel time of 24 hrs shall be provided in case of manpower replacement.

l) Non-availability of OEM back-to-back warranty for supplied systems (hardware and software) during AMC period.

m) Non-compliance of Monitoring functions as specified in 4.**3**.3.3.

n) Non-availability of any of the database modelling tools, display building tools and reporting tools.

o) Online Editing of SCADA, Network and ICCP Database.

p) Non-functioning of complete or individual cube of VPS system.

q) Patch management including Acquisition of security certificate from Certificate Authority, six monthly Security Audit and implementation of the remedial actions suggested by auditor will also be covered under this severity.

r) Incidents specified under severity-1 that are repetitive in nature (happened more than 5 in a quarter) and occurring due to same reason. Such incidents shall be recorded as severity-2 for permanent rectification of the same, irrespective of restoration within specified resolution time in severity-1.

4.6.1.3 Severity-3 (Standard support)

The support services included under this category are when the outage or loss of functionality is neither of an emergency nor priority functionalities as indicated in severity level 1 or 2 above. Problems like database backup and display reworking, required calculations, Failure of DCPC/Terminal server, Support at Control center for the integration of new equipment, failure of any one workstation, printers and integration services as defined in 4.4 during the period of contract including AMC etc. would be covered under this Severity.

Incidents specified under **severity-2** that are repetitive in nature (happened more than 5 in a quarter) and occurring due to same reason. Such incidents shall be recorded as **severity-3** for permanent rectification of the same, irrespective of restoration within specified resolution time in **severity-2.**

4.6.1.4 Severity-4 (General Technical Help)

Request for information, technical configuration assistance, "how to" guidance, and enhancement requests are included under this category.

4.7 Response and Resolution Time

This section describes the target times within which the contractor should respond to support requests for each category of severity. The Initial Response Time is defined as the period from the initial receipt of the support request (through approved communications channels) and the acknowledgment of the contractor subject to the Maximum time defined in Table 4.4. The Action Resolution Time is the period from the acknowledgement of support request to the contractor delivering a solution subject to the Maximum time defined in Table 4.4. This period includes investigation time and consideration of alternative courses of action to remedy the situation. The Action is defined as a direct solution or a workaround.

Complain logging portal with auto escalation functionality is essential before start of Defect Liability Period AMC. Detailed reports along with resolution to be available in the portal. Except for Severity Level 1 & 2 (except manpower availability) all response/resolution times (hours and days) specified below are working hours only.

Table: 4.4 Emergency Support Response/Resolution Time

Severity	Initial Response Time	Action Resoluti onTime	Action
1	30 minutes	1 hours	An urgent or emergency situation requiring continuous attention from necessary support staff until system operation is restored may be by workaround.
2	1 Hours	6 Hours	Attempt to find a solution acceptable to Owner (dependent on reproducibility), as quickly as practical.

3	12 Hours	1 days	Evaluation and action plan. Resolution time is dependent on reproducibility, ability to gather data, and Owner prioritization. Resolution may be by workaround.
4	1 days	5 days	Report on the problem/query is to be furnished.

Following completion of the restoration of operation a "System Operation Restoration Report" shall be completed and signed by the Contractor's responsible engineer. This report shall also be endorsed signed by the Owner responsible engineer and be kept in a file.

The Contractor undertakes the responsibility to organize a system for the remote diagnosis and restoration of malfunctions in the System operation, whenever this is possible, for the purposes of reducing response time and considering all safety measures which must be approved by Owner in order to protect the system and its information. The bidder shall submit the detailed format and procedure for all the activities such as Reporting time, Resolution time, Downtime etc. along with the bid proposal.

4.8 Availability and Maintenance Charges Payment Calculation

It is the endeavor of both the contractor and Owner to maximize system availability to the extent possible. The contractor shall provide guaranteed availability for all supplied systems as specified in Table 4.1. The non-availability hours for availability calculation shall be counted from the end of the allowed Action Resolution time.

A standardized register shall be maintained at each site containing full details of each outages, actions taken by Owner to correct the problem, applicable Severity level, time of reporting to the contractor support engineer/support center pursuant to the appropriate methods in the Agreement, allowed Response time as per the Response times defined in above section, actual Resolution time, and signature of Engineer- in-charge as well as the contractor's support engineer of the site.

Duration of outages over and above the Action Resolution time, as defined in Table 4.4, in each of the Severity levels shall be counted for the non-availability computation and shall be clearly brought out in the register. The resolution may be accepted temporally by a work around, but permanent solution must be provided till then severity will be lowered and such permanent solution shall mark the end of non- availability.

In the event of multiple failures at a site, due to a common cause, the first FPR (Field

Problem Report) logged shall be used for the purpose of availability calculation. However, simultaneous multiple outages due to unrelated cause would be counted separately.

4.8.1 Availability computation for complete SCADA/EMS System and Auxiliary Power Supply System

Availability computation shall be done on per quarter yearly basis per site. The formula to be used for availability computation shall be as under:

$$\text{Availability per quarter yearly (per site)} = \frac{THQ - (S1 \times 1 + S2 \times 0.8 + S3 \times 0.5)}{THQ} \times 100\%$$

Where THQ is Total Hours in the Quarter

S1 is the total non-available hours in Severity Level-1 in the Quarter

S2 is the total non-available hours in Severity Level-2 in the Quarter

S3 is the total non-available hours in Severity Level -3 in the Quarter.

4.8.2 Payment of maintenance charges (based on SCADA/EMS system and Auxiliary Power supply availability)

In the event of availability below a certain level, the maintenance charges would be proportionately reduced as follows:

For complete SCADA/EMS system including Auxiliary Power Supply System

System Availability for each Control Centre perquarter	Deduction as % of the apportioned price of total AMC for complete SCADA/EMS system and Auxiliary Power Supply of the contract applicable for that site(quarterly price)
$\geq$99.99%	NIL
Less than 99.99%	Deduction of 2% of the apportioned price of the quarterly AMC for every 0.5% or part there of decrease in availabilityunder 99.99%. **(**Maximum amount of **Deduction is Limited to 100% of quarterly AMC charges)**

4.8.3 Computation of Availability / Non-availability

The computation of Availability / Non-availability would be rounded up to 2 decimal places at each Contract Co-ordination Site on Quarterly basis and any deduction in the maintenancecharges thereof would be calculated as stated above in Section 4.7.2 on pro-rata basis.

4.9 Contractor's Obligations and Responsibility

The contractor shall guarantee continuous availability of the system as indicated in Table for the defect liability period of one year from the date of operational acceptance. The system availability shall be calculated as indicated above on monthly basis and quarterly basis for contractual purposes.

During this period, the contractor shall take continuous actions to ensure the guaranteed availability. In case the actual availability falls short of the guaranteed availability, it would be considered as contractors default and under the provision of clause GCC 22.8, defect liability period shallbe extended by a period equal to the period / months during which the availability is less than the guaranteed availability. In order to optimize and improve the response of the system, the contractor may re-install the program modules after making the Owner engineer aware of the consequence (like data loss, database rebuild etc.).

Any modification of software/Operating System required to restore functionality due to hardware upgrades/replacement, patches, or arising out of a necessity to fix FPR's (Field problem reports), would be done by the contractor at no extra cost to Owner. The contractor will submit FSR (Field Service Report) and the steps taken to solve the problem, along with details of code changes.

4.10 Detailed Scope of work during Warranty and AMC Period

The detailed scope of services to be provided by Contractor during contract period period **including extension of contract, if any**, shall include but not limited to the following:

i. Contractor shall be responsible for timely compliance of all audits and Vulnerability Assessment (VA) audit observations.

ii. Development and implementation of processes for management and operation including (but not limited to) the following processes:
   - Configuration and Change Management
   - Incident and Escalation management processes
   - Identify, monitor & manage all server resources.

- Tuning for optimum performance
- Daily standard operating procedures
- Reporting metrics and continuous improvement procedures
- Data retention and disposal procedures
- Security Patch management procedure for procured items
- Hardening servers/network devices, in line with security policies.
- Biannual Mock drill of main and backup control centre.

iii. OS Hardening will include activities but not limited to the removal of all non-essential tools, utilities, and services with other system administration by activating & configuring all appropriate security features. Most of the Windows based Operating Systems will include following activities in conjunction to OS hardening guidelines. A preview on the activities associated with Broad categories:

a. Identifying unused or unnecessary ports.
b. Disable/Shut down/remove unused and unnecessary services and daemons.
c. Setting up filters for malicious content for each OS.
d. Test Backup and restoring procedures.
e. Account Policies: Password policy, Account lockout policy etc.
f. Local server Policies: Audit policies, User rights assignments, security options etc.
g. Event logs settings
h. System services
i. Registry settings
j. File & Folder permissions

iv. Contractor shall address all the errors/bugs/gaps in the functionality in the solution implemented at no additional cost during the Project Period.

v. Implement necessary security measures for ensuring the information security of the proposed Solutions.

vi. Administration of its Operating System, including but not limited to management of users, processes, quarterly preventive maintenance and management of servers including updates and patches to ensure that the system is properly updated.

vii. All patches from OEMs shall be implemented by the Contractor ensuring customization done in the solution as per the Owner requirements are applied.

viii. Technical upgrade of the installation to the new version (wherever applicable), as and when required, shall be done by the Contractor. Any version upgrade (in version) of the software / tool / appliance by Contractor to be done after taking prior approval of Owner and after submitting impact assessment of such upgrade at no additional cost to Owner.

ix. Installation and re-installation of the server hardware in the event of system crash/ failures.

x. Management of Data Backup & Retrieval as per the backup policy for applications being hosted, services of virtual machines, Antivirus Management, Resource Monitoring and Reporting for supplied system.

xi. Provide a single-point-of-contact for the resolution of Hardware related problems or to request an equipment upgrade or consultation. If the Hardware supplied by the Contractor is to be replaced permanently, then the Contractor shall replace the equipment of same Make/Model/configuration or of higher configuration.

xii. All engineering changes & support, including but not limited to installation/reinstallation, configuration, integration, testing, commissioning & documentation as may be necessary to match technical and operational specifications of best practices, standards, custom requirements, patches, upgrades or performance improvement of existing equipment, its components or services.

xiii. Proactive and reactive maintenance, repair and replacement of defective components installed under this project. The cost for repair and replacement shall be borne by the Contractor. During Warranty period, replacement of defective components or sub-components shall be replaced by the brand new genuine spare parts bearing the same OEM part number.

xiv. All planned or emergency changes to any component of the system shall be through the approved Change Management process. The Contractor needs to follow all such processes. For any change, Contractor shall ensure:

- Detailed impact analysis.
- Change plan with Roll back plans.
- Appropriate communication on change required has taken place.
- Proper approvals have been received.
- Schedules have been adjusted to minimize impact on the production environment
- All associated documentations are updated post stabilization of the change.

- Version control maintained for software changes. The Contractor shall define the Software Change Management and Version control process document. For any changes to the solution, Contractor has to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. Contractor shall ensure that software and hardware version control is done for entire duration of Contractor's contract.

xv. Maintenance of a log of the performance monitoring of servers including but not limited to following:
  - CPU loading (Peak and Average)
  - Disk utilization (Peak and Average)
  - Operating system error reports
  - Memory utilization (Peak and Average)
  - LAN utilization (Peak and Average)
  - System error log.
  - Backup status
  - Security Log analysis etc.

xvi. Regular analysis of events and logs generated in all the sub-systems including but not limited to servers, operating systems, security devices etc. Proactive measures shall be taken in accordance with the results of the log analysis.

xvii. No extra claim shall be entertained on account of all/part of any job redone on account of Contractor's negligence which results into damages/losses during execution of the job. Also, any component(s) required to meet the smooth functioning of items, after release of Purchase Order shall have to be provided by the successful Contractor. All such cost shall be borne by the Contractor.

xviii. The consumables mentioned anywhere in the documents will include only toners, ink cartridges, printer drums, printer papers, magnetic tapes, and stationery only. No other item will be considered under consumables and repair/replacement of all other parts/items shall be responsibility of the Contractor.

xix. No component(s)/equipment shall be removed from its respective place from the office premises without informing the authorized officials of Owner. A gate-pass duly signed by officer-in-charge or his/her authorized representative is necessary for moving out any parts, for which the Resident/Service Engineer shall maintain appropriate entries in the IN/OUT register and would also co-ordinate in preparing the gate-pass for the same.

xx. One online-portal shall be made available by Contractor where Owner can launch the complaints and it shall keep all records in a database.

xxi. The Contractor shall arrange for standby equipment, if the faulty equipment is not rectified within specified period or machines are taken out of office premises for servicing/repair.

xxii. In case Resident Engineer is not able resolve the issue, Contractor shall assign appropriate resource from his office to resolve the same without any cost implication to the Owner.

xxiii. Required mathematical functions shall be defined in the supplied system as and when required by owner.

xxiv. Security including anti-virus administration and management service shall ensure a secure data centre environment through implementation of appropriate security policies. This service includes:

- Addressing the ongoing needs of security management including, but not limited to, configuration and monitoring of various devices/ tools such as firewall, intrusion detection, Host based Intrusion Prevention (HIPS), APT, content filtering and blocking, virus protection, malware protection and vulnerability protection through implementation of proper patches and rules.
- Ensuring that latest updates/patches etc. for identified vulnerabilities. Ensure all antivirus and other information security agents across the network are always updated with latest signatures files as and when released by the OEM within specified time line,
- Respond to security breaches or other security incidents and coordinate with respective OEM in case if a new threat is observed to ensure that patch is made available for the same.
- Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, protecting email gateways, firewalls, servers from viruses.
- Detect, analyze and report critical security alerts on a real-time basis.
- Vulnerability assessment of network and security services, servers and desktops and remediation of the same.
- Periodic cross-checking of security policy compliance.

xxv. **MIS Reports**: Contractor shall submit the reports on a regular basis in a mutually decided format. The following reports as a minimum shall be submitted:

- **Monthly reports**

  - Component wise server as well as Virtual machines availability and resource utilization
  - (non)- conformance report, if any.
  - Summary of component wise uptime.
  - Log of preventive / scheduled maintenance undertaken
  - Log of break-fix maintenance undertaken
  - All relevant reports required for calculation of system availability.
  - Change Management Reports.
- **Quarterly Reports**
  - Consolidated component-wise availability and resource utilization.
  - All relevant reports required for calculation of system availability.

4.11 Responsibilities of Owner

The responsibilities of the Owner during the maintenance period are as follows: -

(a)Owner shall ensure that proper Environmental conditions are maintained for the system.

(b)Owner shall ensure that the System is kept and operated in a proper and prudent manner as described in the system documentation provided by the Contractor and only trained Owner representatives (or persons under their supervision) are allowed to operate the system.

(c)The owner shall provide access to the sites of installation for purposes of providing Support Services.

(d)The owner shall provide the contractor with Space for Office and storage for their maintenance staff and spares.

4.12 Scope of Maintenance of new RTUs and Associated Items

4.12.1 Introduction

This project scope includes the maintenance of the RTU & associated items (RTU & Associated Cards, LDMS, MFT, CMR, HDR, OLTC, Weather Sensor etc. and other associated cabling) supplied under this project at different locations across the Eastern Region. **The above scope also covers maintenance of integrated new bay extension (MFT, CMR, HDR, OLTC etc. and other associated cabling) in the supplied RTU under this project during entire project life cycle.** These RTUs shall provide data to the respective RLDC/SLDC/Sub SLDC.

The scope of maintenance includes the following types of maintenance.

a) Preventive Maintenance
b) Breakdown Maintenance
c) Integration & reconfiguration work

This section consists of scope of work of the contractor to maintain the equipment (RTU & associated items) in case a fault is reported and also to keep the equipment in proper operating condition. The scope of Comprehensive maintenance includes fault finding, repair or replacement of defective parts, supply of spare components and functional checking in coordination with respective RTU reporting control centers. The Contractor shall use his own testing instruments/ tools/ any other item required for maintenance of equipment. If any special testing equipment/s is/are required for testing and repair of the system, same shall be arranged by the contractor. The contractor shall arrange any other materials, required to maintain the RTU which is not specifically mentioned in this scope. Contractor will take all due necessary safety precautions for proper safety of man & machine while carrying out the work at site. The contractor will also be required to take necessary insurance cover for the personnel deputed for the work covered under this contract. The owner shall have no responsibility whatsoever for claims arising out of negligence/accident or any other reason for the personnel employed by the contractor.

4.12.2 Reporting of faulty/ Service request

Immediately on noticing the fault, the fault will be reported by the Owner on Call Tracking system/phone/fax/e mail to the contractor and the details will be informed as per approved format. The fault reporting time on phone shall be taken as reference time for the purpose of Response time (RT) and up time (UT).

4.12.3 Response Time & Uptime

Contractor shall depute his engineer so as to reach site within 12 Hrs. of the fault reporting time. This RT is in case of RTU not reporting to control centre. The response time for other type of faults (Analog/Digital data not coming correct/Data validation) shall be 24 Hrs. Uptime/rectification time of the fault shall be 4 Hrs. after access to the site. The contractor engineer shall carry the components which may be required for rectification of the fault based on the preliminary inputs from the repairing site.

Contractor's services must be available on phone or fax round the clock on all working days/holidays for fault reporting and corrective actions. Emergency calls will be attended with utmost priority keeping aside any protocol and obligations.

Contractor shall nominate two (02) qualified and experienced engineer/ official at Sikkim SLCD & JUSNL SLDC for maintenance of RTU supplied for Sikkim & JUSNL. This however, does not relieve contractor for assessing their actual manpower requirement more than specified above, for rectification of fault within the stipulated Response Time and Up Time. The AMC Engineers shall be solely responsible for coordination with all its service engineers available at various sites for rectification of faults. The Engineer shall be adequately supported by technical staff for quick restoration of the system. Engineer shall arrange for adequate transportation/accommodation for their staff as per work demand. All Contractors' staff should be equipped with necessary tools kit, testing instruments and mobile phones.

4.12.4 Scope of work

A. Preventive Maintenance

The Contractor will carry out semiannual preventive maintenance visits at all RTU locations. The work during preventive maintenance includes following activities.

(a) Physical inspection of RTU to check physical damage, cleanliness, rat droppings, lizard or other vermin and take corrective actions as required.
(b) Preventive measures like blowing and cleaning for removal of dust from RTU panel, tightening of all power and signal connections in RTU/SIC/Control & Relay panels.
(c) Checking up of environmental conditions and report any abnormality to customer for necessary corrective action by them.
(d) Checking MFT/CMR's output for any suspected/bad input values
(e) Tightening of all the power and control connections
(f) Checking of earthing & recommendation to improve the same if required
(g) Checking of DC Voltage
(h) Checking for all Telemetered Parameters
(i) Checking for AC Voltage L-L, L-N
(j) Repair & Replacement of Faulty Cards/Modules (CPU, PSU, AI, DI, DO, MFT, CMR, HDR, MODEM, etc.) as per requirement
(k) Plan for preventive measure to arrest recurrence of such faults.

Cyber security preventive maintenance for RTU & LDMS

(a) Firmware update/upgrade of RTU

(b) Patching of application/service software of RTU

(c) Update of OS, service/application software in associated system like PCMT, LDMS, etc.

(d) Updating of other software tools like protocol analyser, etc.

(e) Vulnerability disclosure and its mitigation by the vendor

B. Breakdown Maintenance

Break down Maintenance is to be carried out in the event of malfunctioning / non-reporting of RTUs / cards, which affects the normal operation of the RTU. The scope of work during breakdown maintenance includes the following activities.

(a) Rectification of fault.
(b) Contractor shall replace faulty cards/modules (CPU, PSU, AI, DI, DO, MFT, MODEM, CMR, HDR etc.) or equipment identified during the maintenance.
(c) Contractor shall check the configuration & setting of replaced component and outputs for correctness of parameters being telemetered.
(d) Contractor shall replenish the spares, either by a new one or by repairing, if feasible
(e) Analysis report of the fault

C. Integration of new bays & reconfiguration

The scope of work under Integration of new bays & reconfiguration work includes-

(a) Material such as CPU, PSU, AI, DI, DO, MFT, MODEM, CMR, HDR and any other material required for additional bay integration during AMC shall be provided by Contractor for RTUs installed at various locations.
(b) Integration work of additional bay with RTU during AMC
(c) Checking /re-configuration of MODEM/s at RTU and control centre ends.
(d) Downloading of database files and updating of new database in the RTU for additional bay integration work
Further, integration of new Bays shall not be treated as new RTU integration during AMC period, and any such bay extension during AMC shall be in the scope of the contractor **The cost of new bay integration shall be inclusive in the Annual Maintenance charges**.

D. Reports submission during Maintenance

(a) Any activity carried out shall be recorded for all the visits and activities carried out during AMC period shall be maintained by the contractor and monthly report for all such activities shall be submitted to POWERGRID and constituents in review meetings.

(b) Contractor shall document the maintenance activities carried out and shall establish a maintenance record for the performance of their duties and location wise history record of the equipment for future reference.

Three copies of monthly report shall be submitted to Owner.

4.12.5 Responsibilities of Owner in case of RTU

The responsibilities of the owner during the maintenance period are as follows:

(a) Owner shall nominate an Engineer I/C who shall be sole coordinator and interface between Owner and the Contractor.

(b) Owner shall arrange security passes/ permissions required by Contractors' maintenance engineers for all sites.

(c) Owner shall ensure free and unrestricted access to equipment sites during the maintenance period to the vendor's personnel and /or authorized personnel working on behalf of contractor.

(d) Owner shall provide to the contractor with the information on any planned expansion, alteration or relocation of the equipment that may have the impact on the system under maintenance.

(e) Owner shall provide following information in the prescribed format as fault reporting procedure.

i) Indication of LEDs in RTU panel (on the cards and modems)
ii) Status of communication link
iii) Healthiness of 48 V DC supply to the RTU panels
iv) MCB positions in the RTU

On receipt of these information contractor shall depute their personnel at site. Fault reporting time shall start after requisite information in duly filled up FORMAT is informed to the contractor by CTS/Fax/e-mail/phone. Contractor's engineer shall reach within 24 hours of fault reporting at fault site for the fault where RTU is not reporting to control centre and within 36 hours of reporting for other type of faults for e.g. anomaly in analogue or digital values etc. Contractor's personnel shall restore the RTU reporting within 6 hours of reaching at site failing which penalty shall start.

4.12.6 Penalty Clause for RTU & associated items

Contractor will maintain the system as per above defined Response Time and Up Time failing which Rs 2000 per four hours of delay subject to the maximum of Rs 5000 per day for every breach will be deducted by Owner from the amount due to contractor for maintenance.

4.13 Annual Training during AMC Period

The Contractor shall provide yearly training on complete system for 5 Days for 20 owner's personnel and 10 Employer's personnel during entire period of AMC. This training shall cover any/all modules as per **Table 2.1** (Part A; Sec-2), to be finalized during as and when required.

4.14 Responsibility Matrix

The table in this section provides a summary definition of the roles and responsibilities of the contractor and Owner

Legend:

● This indicates who has primary responsibility to perform this function.

A This indicates who will provide assistance.

Table 4.5 Responsibility Matrix

Item	Task	Owner	Contractor
1.0	**PROBLEM IDENTIFICATION**		
1.1	Root cause analysis to determine whether the fault is attributable to Hardware or Software.	----	●
1.2	Resolution of problems involving third party maintainer where there is uncertainty whether the root cause is hardware or software.	----	●
2.0	**SOFTWARE PROBLEM RESOLUTION**		
2.1	Report problem and assist with problem identification.	----	●
2.2	Provide or recommend corrections, temporary patches, workarounds or other fixes to system problems.	----	●
2.3	Install and test corrections, temporary patches,workarounds or other fixes to	----	●

	system problems.		
3.0	**ROUTINE SOFTWARE SUPPORT**		
3.1	Build and maintain database, displays and reports.	A	●
3.2	Perform system back-ups.	----	●
3.3	Restore or reinstall software from back-ups.	----	●
3.4	Monitor system logs (part of remote monitoringservice)	----	●
3.5	Maintain system (Hardware, Software, Network etc.) logs	----	●
3.6	Maintain user accounts	●	**A**
4.0	**HARDWARE PROBLEM RESOLUTION**		
4.1	Report problem and assist with defining problem	●	**A**
4.2	Troubleshoot problem to diagnose if it is software-related or hardware-related	----	●
4.3	Identify failed component, replace failed components in the system using parts from spares inventory	----	●
4.4	Restore operation of repaired/replaced equipment	----	●
5.0	**HARDWARE SPARE PARTS**		
5.1	Manage local spares inventory	----	●
5.2	Replenish local spares inventory	----	●
6.0	**INTEGRATION AND DATABASE WORK AT CONTROL CENTRE END**		
6.1	RTU/DCPC/TERMINAL SERVER Integration	----	●
6.2	ICCP Integration	----	●
6.3	WAMS/REMC/Other application integration	----	●
6.4	Database and Display	A	●
7.0	**AUXILIARY POWER SUPPLY SYSTEM/DG SET**		
7.1	Troubleshoot problem to diagnose	----	●
7.2	Replenish local spares inventory	----	●

8.0	**CYBER SECURITY MONITORING**		
8.1	Patch/Signature/Update/firmware Updates	----	●
8.2	Cyber Security Monitoring	A	●
8.3	Six monthly Audits	----	●
8.4	Implementation of Recommendations during Audit	----	●
8.5	Implementation of Monitoring and compliance manager for Critical Infrastructure Protection	●	●
8.6	Maintenance of Spares	----	●
9.0	**RTU MAINTENANCE**	----	●
10.0	**VPS & VC MAINTENANCE**	**----**	●

DG SET MAINTENANCE FORMAT

DG SET MAINTENANCE FORMAT TO BE FILLED AT SITE
SITE INFORMATION:-
SITE NAME :-
ADDRESS :-
TELEPHONE AND FAX NO:-

SL. NO.	DESCRIPTION	VALUE, IF ANY	REMARKS
1.	Physical Inspection		
2.	Visual Inspection & Rectification of leakage in cooling, oil, fuel, air & exhaust system		
3.	Cleaning has been done		
4.	Power connections checked for over heating		
5.	Control Connections are all tight		
6.	All indications on the panel are working		
7.	Inspection & adjustment of belts tension of fan, water pump & charging alternator		
8.	Inspection of vibration damper for wobble & eccentricity.		
9.	Testing coolant for its proper PH & PPM Value to avoid rusting, corrosion & erosion of internal engine components.		
10.	Testing fuel manifold pressure of PT Pump (Fuel pump), whenever required.		
11.	Inspecting end plays of crankshaft, accessory drive, turbo charger etc.		
12.	Inspection & adjustment of plunger travel for injectors & tapped clearance for proper fuel injection & valve timing.		
13.	Inspection & maintenance of carbon brushes and slip rings (if applicable).		
14.	Performing insulation check of alternator/ Greasing of alternator bearings. (Whenever required/4500 hours of running)		
15.	Inspection of earthing systems.		
16.	Inspection of all relays, timers, ACB & contactors for any kind of malfunctioning.		
17.	Inspection of fault tripping systems		

SL. NO.	DESCRIPTION	VALUE, IF ANY	REMARKS
18.	Inspection of all safety controls viz. Low Lube Oil Pressure, High Water Temperature & Over Speed Safety (if applicable).		
19.	Functional checks of starting circuits/starting motor and charging alternator		
20.	Testing & recording performance parameters of the DG set in loaded condition.		
21.	Battery charge voltage		
22.	Water level in battery		
23.	Condition of Belt		

Format A: UPS/ACDB MAINTENANCE FORMAT

SL. NO.	DESCRIPTION	VALUE, IF ANY	REMARKS
1	UPS & ACDB Cleaning has been done		
2	Power connections checked for tightness & over heating		
3	Control Connections are all tight		
4	All indications on the panel are working		
5	All cooling fans are working		
6	Checking for AC Voltage L-L, L-N		
7	Checking for input AC current		
8	Checking for Input frequency		
9	Checking of DC Voltage		
10	Checking AC output Current		
11	Checking for O/P frequency		
12	Rectifier LED		
13	Inverter LED		
14	Static Switch LED		
15	Normal Operation & link status as per manufacturer recommendations/ performance		
16	Battery Current Limit		
17	Float voltage		
18	Invertor Voltage		
19	Invertor frequency		
20	Indication Bulbs Of ACDB		
21	Checking for transfer, of UPS to Bypass and Bypass to UPS		
22	Checking for UPS transfer to batteries		
23	Checking of earthing		
24	Battery Voltage, Resistance Impedance measurement done and details enclosed		
25	Parameter checked in SCADA System		
26	Proper guidance given for normal day to day activities		
27	Check Functioning of hooter		

Remarks from Customer/Contractor: -

Contractor's Representative **Owner's Representative**

DC Power Supply Equipment Maintenance Format

Format

DC POWER SUPPLY EQUIPMENT MAINTENANCE FORMAT TO BE FILLED AT SITE

SITE INFORMATION

SITE NAME : ____

ADDRESS : ____

_ --

TELEPHONE AND FAX NO --

	DESCRIPTION	VALUE,IF ANY	REMARKS
1	Cleaning done		
2	Power connections checked for tightening & over heating		
3	Control Connections are all tight		
4	All indications/meters/display on the panel are working		
5	Input frequency		
6	Rectifier LEDs		
7	Normal Operation on each module		
8	Float voltage		
9	Checking for ripple Voltage		
10	Checking for AC Voltage L-L, L-N		
a	R - Y		
b	Y - B		
c	R - B		
11	Checking AC Current		
12	Checking of DC Voltage		
13	Checking of earthing		
14	Battery voltage/resistance measurement done & enclosed		
15	Load test done on batteries as enclosed		
16	Check functioning of hooter/Buzzer (Alarm Annunciation)		
17	Parameters checked in SCADA system		
18	Proper guidance given for normal day to day operation.		

Suggessions from Contractor :

Remarks from Customer :

CONSTITUENT/POWERGRID representative

……End of Section-4……

Vol. II, Part-A
Appendix - A Existing RTU Details

A. DVC

S. No.	RTU Location/Station	Number Of Analogs data points in the RTU	Number Of Digital data points in the RTU	Make	Existing Control Centre name to which RTU reports presently (i.e. Sub-LDC or SLDC or RLDC)	Communication Interface at RTU side	Existing Interface at Control Center		Proposed Interface at Control Center		Proposed Interface at Backup Control Center	
							Port at CFE	No. of Channels	Port at CFE	No. of Channels	Port at CFE	No. of Channels
1	ASPN__DV	41	91	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:199 ; Standby Channel:200)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.	
2	BURNP_DV	46	84	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:105 ; Standby Channel:106)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.	
3	BIADA_DV	40	84	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:115 ; Standby Channel:116	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.	

							)				
4	BTPS__DV	121	300	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:175 ; Standby Channel:176)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
5	BELMU_DV	47	120	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:161 ; Standby Channel:162)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
6	BARHN_DV	60	131	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:185 ; Standby Channel:186)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
7	BRDWN_DV	104	203	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:111 ; Standby	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							Channel:112)				
8	BARJN_DV	85	169	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:117 ; Standby Channel:118)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
9	CHAND_DV	27	81	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:125 ; Standby Channel:126)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
10	CTPBN_DV	50	133	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:173 ; Standby Channel:174)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
11	CTPS1_DV	144	379	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:181 ; Standby	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							Channel:182)				
12	CTPSA_DV	54	144	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:113 ; Standby Channel:114)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
13	GOLA__DV	51	124	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:137 ; Standby Channel:138)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
14	DHANB_DV	148	562	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:149 ; Standby Channel:150)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
15	DTPS__DV	147	385	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:179 ; Standby	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							Channel:180)				
16	DURGN_DV	110	190	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:197 ; Standby Channel:198)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
17	GIRID_DV	66	372	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:151 ; Standby Channel:152)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
18	HAZAR_DV	30	72	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:131 ; Standby Channel:132)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
19	HWRHN_DV	30	96	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:183 ; Standby	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							Channel:184)				
20	JAMUR_DV	50	117	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:101 ; Standby Channel:102)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
21	JMSHN_DV	71	184	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:127 ; Standby Channel:128)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
22	KODER_DV	44	113	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:171 ; Standby Channel:172)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
23	KHARG_DV	25	73	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:141 ; Standby	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							Channel:142)				
24	KLYNS_DV	106	225	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:167 ; Standby Channel:168)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
25	KLIPN_DV	67	130	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:107 ; Standby Channel:108)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
26	KOLGN_DV	21	62	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:129 ; Standby Channel:130)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
27	KMRDN_DV	60	137	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:103 ; Standby	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							Channel:104)				
28	MATHN_DV	73	185	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:169 ; Standby Channel:170)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
29	MEJAN_DV	148	345	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:177 ; Standby Channel:178)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
30	MOSBN_DV	48	114	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:135 ; Standby Channel:136)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
31	NIMIA_DV	44	115	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:145 ; Standby	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							Channel:146)				
32	NORTH_DV	36	90	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:147 ; Standby Channel:148)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
33	PURUL_DV	41	91	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:123 ; Standby Channel:124)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
34	PNCHT_DV	48	116	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:163 ; Standby Channel:164)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
35	PRULN_DV	86	171	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:165 ; Standby	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							Channel:166)				
36	TISCO_DV	14	54	SCHNEIDER SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:153 ; Standby Channel:154)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
37	MEJIB_DV	24	193	AREVA /SCHNEIDER SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 1 Main ; Gateway 1 Port 2 Standby (Main Channel:187 ; Standby Channel:188)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
38	DSTPS_DV	32	178	AREVA /SCHNEIDER SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:155 ; Standby Channel:156)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
39	KODAM_DV	54	311	SIEMENS SAS	Main - Maithon	IEC 101 /PDH/ OPGW	TS-2 /Port 13 channel-26	1	IEC 104 /OPGW	2	As per general guidelines of statutary body/apex for Eastern Region.
40	RAGHU_DV	72	213	ABB SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for

							Port 1 Standby (Main Channel:195 ; Standby Channel:196)				Eastern Region.
41	PUTKN_DV	103	215	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:109 ; Standby Channel:110)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
42	PTHRN_DV	109	227	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:119 ; Standby Channel:120)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
43	PATRN_DV	57	127	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:133 ; Standby Channel:134)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
44	RAMKA_DV	24	76	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							Standby (Main Channel:121 ; Standby Channel:122)				
45	RAMG1_DV	76	145	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 1 Main ; Gateway 1 Port 2 Standby (Main Channel:189 ; Standby Channel:190)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
46	RAMG2_DV	50	131	GE SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 2 Port 2 Main ; Gateway 2 Port 1 Standby (Main Channel:191 ; Standby Channel:192)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
47	BK400_DV	26	139	AREVA /SCHN EIDER SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby (Main Channel:157 ; Standby Channel:158)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.
48	KONAR_DV	32	90	RTU Rams daq	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Node 1 SYS/BUS B Main ; Node 2 SYS/BUS A Standby	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

							(Main Channel:193 ; Standby Channel:194)				
49	KODAM_220	47	293	SIEMENS SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 1 Main ; (Main Channel:139)	1	IEC 104 / OPGW	2	As per general guidelines of statutary body/apex for Eastern Region.
50	DSTPS_220	14	50	AREVA /SCHNEIDER SAS	Main - Howrah Standby - Maithon	IEC 104 / OPGW	Default: Gateway 1 Port 2 Main ; Gateway 1 Port 1 Standby (Main Channel:71 ; Standby Channel:72)	2	As per Existing	As per Existing	As per general guidelines of statutary body/apex for Eastern Region.

B. WBSETCL

S. No.	RTU Location/Station	Number Of Analogs data points in the RTU	Number Of Digital data points in the RTU	Make	Existing Control Centre name to which RTU reports presently (i.e. Sub-LDC or SLDC or RLDC)	Communication Interface at RTU side	Existing Interface at Control Center		Proposed Interface at Control Center		Proposed Interface at Backup Control Center	
							Port at CFE	No. of Channels	Port at CFE	No. of Channels	Port at CFE	No. of Channels
1	ARAMBAG 400 kv	86	254	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
2	ASANSOL 220 kv	31	107	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
3	ASHOKNAGAR 132 kv	23	71	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
4	BARASAT 132 kv	22	72	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
5	BISHNUPUR OLD 132kv	27	82	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
6	BONGA 132 kv	19	66	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
7	DOMJUR 220 kv	43	141	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
8	DPL TPS	79	209	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
9	DURGAPUR 220 kv	59	202	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
10	GOKORNA 220 kv	57	188	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
11	HALDIA NEW 220 kv	32	112	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

12	HALDIA OLD 132 kv	27	83	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
13	HOWRAH 220 kv	58	174	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
14	JEERAT 400 kv	92	297	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
15	JOKA 132 kv	24	80	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
16	KASBA 220 kv	44	153	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
17	KHARAGPUR (HIZLI) 132 kv	23	76	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
18	KOLAGHAT	22	69	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
19	Kolaghat TPS (KTPS)	98	273	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
20	LAKSHIKANTA PUR	53	125	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
21	LILUAH	41	112	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
22	MIDNAPUR	50	164	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
23	PURULIA PUMP STORAGE (PPSP)	30	69	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
24	PURULIA	29	87	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
25	RISHRA	58	166	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
26	SALTLAKE AIS	23	67	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

27	SATGACHIA	49	157	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
28	SIANTHIA	17	61	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
29	TITAGARH	26	74	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
30	ALIPURDUAR	11	48	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
31	BIRPARA	25	71	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
32	CHALSA	35	113	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
33	GANGARAMPUR	17	51	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
34	Malda	27	85	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
35	NBU	36	88	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
36	NEW JALPAIGURI (NJP)	47	143	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
37	RAIGANJ	27	73	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
38	RAMAM	13	58	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
39	TCF-1	25	71	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
40	TCF-2	26	75	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
41	TCF-3	27	76	M/S ALSTOM	MCC-Howrah & BCC- Abhikshan	Terminal server/PDH	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

42	ADISAPTAGRAM	27	71	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
43	Amtala	68	158	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
44	Bagmundi	29	56	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
45	Bagnan	50	78	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
46	Balurghat	51	126	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
47	Bankura	84	188	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
48	Barjora	62	132	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
49	Bashirhat	56	124	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
50	Belmuri	50	120	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
51	Berhampur	76	169	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
52	Bighati	56	124	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
53	Birsingha	62	137	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
54	Bolpur	73	158	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
55	C.K. Road	72	158	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
56	Chanditala	62	137	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

57	Chanditala400	136	387	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
58	Contai	53	122	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
59	Coochbehar	57	129	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
60	Dalkhola	84	190	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
61	Debagram	72	162	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
62	Dharampur	66	71	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
63	Dhulian	34	77	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
64	DPL II	53	161	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
65	Durgapur400	42	118	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
66	Egra	73	147	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
67	Falta	75	153	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
68	Food Park	68	146	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
69	Foundary Park	94	178	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
70	HaldiaNIZ	59	141	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
71	Hura 220	93	213	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

72	Jangipara	47	111	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
73	Jhargram	56	128	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
74	JHP Stage-I	31	65	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
75	JHP Stage-II	42	101	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
76	Kakdwip	56	128	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
77	Kalimpong	21	65	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
78	Kalna	38	91	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
79	Kalyani	66	115	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
80	Katwa	91	201	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
81	Khanyan	44	106	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
82	Kharagpur 400	137	349	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
83	Kharagpur WB IDC	65	143	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
84	Khatra	50	120	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
85	Khejuria	50	116	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
86	KLC (Bantala)	107	231	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

87	Krishnanagar	120	276	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
88	Kuli	59	85	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
89	Kurseong	43	94	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
90	Lalgola	50	120	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
91	Lebong(Darj)	38	84	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
92	Mahachanda	60	141	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
93	Mankar	63	155	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
94	Mathabhanga	50	116	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
95	Mohishpota	44	106	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
96	Moinaguri	71	170	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
97	Najirpur	44	102	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
98	New Bishnupur	122	305	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
99	New Town AA-1	74	252	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
100	New Town AA-3	147	314	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
101	Pingla	60	139	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

102	Raghunathganj	54	113	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
103	Raghunathpur	58	129	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
104	Raina	56	123	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
105	Rampurhat	53	119	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
106	Ranaghat	93	192	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
107	Saltlake GIS	188	856	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
108	Samsi	56	127	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
109	Siliguri	50	118	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
110	Sirakol	44	105	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
111	Sonarpar	45	118	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
112	Subhasgram	128	294	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
113	Tamluk	65	144	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
114	Ukhra	65	138	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
115	Uluberia	78	180	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
116	Vidyasagar	82	217	M/S Chemtrol s	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

117	NEW ALIPURDUAR 220 kv	57	116	M/S Siemens	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
118	BARASAT 220 kv	26	47	M/S Siemens	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
119	BHADRAPUR 132 kv	182	605	M/S ZIV	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
120	DEBRA GIS 132 kv SAS	126	545	M/S GE	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
121	Dharampur-II 220 kv	105	503	M/S Schneider	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
122	DINHATA 132 kv	188	561	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
123	GAZOLE 220 kv	555	1651	M/S Siemens	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
124	GOKARNA 400 kv	93	226	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
125	HARISCHANDRA	513	1145	M/S ZIV	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
126	Hind Motor	13	29	RTU not available	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
127	INDUS 132 kv	210	766	M/S ZIV	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
128	JEERAT SAS	12	36	M/S GE	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
129	JHALDA	111	35	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
130	MOHITNAGAR	262	665	M/S ZIV	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
131	NEW SAGARDIGH	204	896	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

132	NPPSP	30	106	M/S Siemens	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
133	PANAGARH	170	1196	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
134	REJINAGAR	679	1173	M/S GE	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
135	SADAIPUR	86	360	M/S ABB	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
136	SALAR	274	154	M/S Chemtrols	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
137	SALTL STADIUM SAS	229	1040	M/S GE	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
138	SONAKHALI	232	947	M/S ZIV	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
139	TRKSWAR	16	72	M/S NELCO	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
140	BAKRESWAR TPS (BKTPS)	58	136	M/S GE	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
141	Bandel TPS	247	89	M/S ABB	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
142	DALMIA	90	11	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/Lease network	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
143	Hiraonmoy energy LTD	108	68	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/Lease network	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
144	JK Nagar	71	40	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/Lease network	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
145	JSW	10	0	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/Lease network	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
146	SAGARDIGHI TPS	88	181	M/S GE	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

147	Santaldih TPS (STPS)	153	129	M/S GE	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
148	TLDP3	22	35	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/Lease network	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
149	TLDP4	24	36	not known	MCC-Howrah & BCC- Abhikshan	IEC-101/TS/Lease network	**FEP LAN**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
150	HALCP (TATA POWER)	18	24	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/Lease network	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
151	RAILWAY	243	63	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/Lease network	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
152	URTDSM	174	0	M/S GE	MCC-Howrah & BCC- Abhikshan	IEC-104/LAN	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
153	Baruipur 220 kv	63	168	not known	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**
154	Manbazar 132 kv GIS	110	598	M/S GE	MCC-Howrah & BCC- Abhikshan	IEC-104/SDH	**FEP Router**	**2**	**Through Firewall**	**2**	**Through Firewall**	**2**

C. OPTCL

S. No.	RTU Location/Station	Number of Analogs data points in the RTU	Number of Digital data points in the RTU	Make	Existing Control Centre name to which RTU reports presently (i.e. Sub-LDC or SLDC or RLDC)	Communication Interface at RTU side	Existing Interface at Control Center		Proposed Interface at Control Center		Proposed Interface at Backup Control Center	
							Port at CFE	No. of Channels	Port at CFE	No. of Channels	Port at CFE	No. of Channels
1	JAYAN_GR	71	191			TS	IEC101					
2	BALIM_GR	32	95			TS	IEC101					
3	MACHK_GR	42	62			ROUTER	IEC104					
4	UPKLB_GR	41	59			TS	IEC101					
5	RAYAG_GR	58	54			ROUTER	IEC104					
6	THERU_GR	41	52			TS	IEC101					
7	INDRA_GR	61	148			TS	IEC101					
8	KESIN_GR	29	91			TS	IEC101					
9	BHANJ_GR	45	56			TS	IEC101					
10	NAREN_GR	86	121			ROUTER	IEC104					
11	BERAH_GR	38	61			TS	IEC101					
12	CHATR_GR	52	62			ROUTER	IEC104					

13	ASKA_GR	52	78			TS	IEC101						
14	AKUSI_GR	22	54			TS	IEC101						
15	BHUBA_GR	25	58			TS	IEC101						
16	CHAND_GR	97	118			ROUTER	IEC104						
17	NAYAG_GR	44	37			ROUTER	IEC104						
18	KHURD_GR	23	60			TS	IEC101						
19	PURI__GR	46	41			ROUTER	IEC104						
20	CUTTA_GR	21	81			TS	IEC101						
21	CHOUD_GR	42	41			ROUTER	IEC104						
22	ICCL__GR	13	24			ROUTER	IEC104						
23	BIDAN_GR	80	89			ROUTER	IEC104						
24	SIJUA_GR	50	41			ROUTER	IEC104						
25	MENDH_GR	147	218			TS	IEC101						
26	MERAM_GR	154	273			TS	IEC101						
27	TTPS_GR	69	157			TS	IEC101						
28	NALCO_GR	49	140			TS	IEC101						
29	RENGA_GR	24	73			TS	IEC101						
30	REGSS_GR	15	69			TS	IEC101						
31	CHAIN_GR	36	92			TS	IEC101						

32	RAIRA_GR	20	44			TS	IEC101					
33	JODA__GR	79	134			TS	IEC101					
34	BARIP_GR	25	48			TS	IEC101					
35	DUBNW_GR	53	168			TS	IEC101					
36	DUBOL_GR	67	143			TS	IEC101					
37	PARAD_GR	69	131			TS	IEC101					
38	JAJPU_GR	88	115			ROUTER	IEC104					
39	BHADR_GR	57	114			TS	IEC101					
40	BALAS_GR	58	118			TS	IEC101					
41	ANGUL_GR	31	62			TS	IEC101					
42	BOIND_GR	27	60			TS	IEC101					
43	KENDR_GR	69	83			ROUTER	IEC104					
44	KAMAK_GR	25	51			TS	IEC101					
45	BUDHI_GR	88	213			TS	IEC101					
46	BURLA_GR	55	119			TS	IEC101					
47	IBTPS_GR	57	98			TS	IEC101					
48	BOLNW_GR	33	109			TS	IEC101					
49	ROURK_GR	55	59			ROUTER	IEC104					
50	BURL1_GR	41	102			TS	IEC101					

51	CHIP2_GR	34	60			TS	IEC101					
52	SAMBA_GR	55	96			ROUTER	IEC104					
53	RAJGA_GR	45	55			ROUTER	IEC104					
54	TARKE_GR	51	170			TS	IEC101					
55	BOLOL_GR	20	60			TS	IEC101					
56	BARGA_GR	29	60			TS	IEC101					
57	BARKO_GR	20	47			TS	IEC101					
58	MISHR_GR	10	25			ROUTER	IEC104					
59	BSL___GR	41	69			TS	IEC101					
60	SHYAM_GR	21	23			ROUTER	IEC104					
61	MGM__GR	8	31			TS	IEC101					
62	BPPL__GR	25	62			ROUTER	IEC104					
63	GURUD_GR	9	16			ROUTER	IEC104					
64	LAXMI_GR	47	65			ROUTER	IEC104					
65	UAIL__GR	25	38			ROUTER	IEC104					
66	PURUS_GR	29	38			TS	IEC101					
67	KHAJU_GR	31	53			TS	IEC101					
68	CHNDB_GR	75	88			ROUTER	IEC104					
69	SALIV_GR	9	9			ROUTER	IEC104					

70	ACC___GR	11	11			ROUTER	IEC104							
71	ARYAN_GR	17	46			TS	IEC101							
72	TATPW_GR	80	103			ROUTER	IEC104							
73	STERL_GR	69	288			ROUTER	IEC104							
74	SAMAG_GR	106	122			ROUTER	IEC104							
75	LAPN2_GR	71	118			ROUTER	IEC104							
76	KESN1_GR	26	12			ROUTER	IEC104							
77	JSL___GR	11	31			TS	IEC101							
78	TUSR1_GR	25	9			ROUTER	IEC104							
79	NBVL__GR	35	20			TS	IEC101							
80	BHOGR_GR	29	47			TS	IEC101							
81	TUSR2_GR	25	9			ROUTER	IEC104							
82	JABAM_GR	14	14			TS	IEC101							
83	MUNGI_GR	12	8			TS	IEC101							
84	TSIL__GR	9	37			TS	IEC101							
85	HINDA_GR	43	58			ROUTER	IEC104							
86	VEDAN_GR	45	92			TS	IEC101							
87	KUCHI_GR	63	76			ROUTER	IEC104							
88	ADHUN_GR	13	50			TS	IEC101							

89	BRG__GR	13	14			TS	IEC101					
90	ARATI_GR	42	43			TS	IEC101					
91	VISA__GR	18	9			TS	IEC101					
92	PPT__GR	30	29			TS	IEC101					
93	ULTRA_GR	8	8			ROUTER	IEC104					
94	AISCL_GR	19	22			TS	IEC101					
95	IMFAA_GR	32	36			TS	IEC101					
96	JSPL__GR	18	38			TS	IEC101					
97	MINAK_GR	23	17			TS	IEC101					
98	OCL___GR	12	40			ROUTER	IEC104					
99	VEDA1_GR	24	48			TS	IEC101					
100	OPCL__GR	22	43			TS	IEC101					
101	BPSL__GR	102	77			TS	IEC101					
102	BRPL__GR	9	31			TS	IEC101					
103	MIL___GR	24	31			TS	IEC101					
104	JSPLA_GR	71	188			TS	IEC101					
105	RSP___GR	41	39			TS	IEC101					
106	OCLRJ_GR	43	59			TS	IEC101					
107	GMR___GR	47	57			TS	IEC101					

108	PPL___GR	19	37			TS	IEC101					
109	ESSAR_GR	40	15			TS	IEC101					
110	FACOR_GR	15	22			TS	IEC101					
111	JCL___GR	11	24			TS	IEC101					
112	BANGI_GR	33	4			TS	IEC101					
113	ADITY_GR	56	94			TS	IEC101					
114	OPTCL_GR	45	84			ROUTER	IEC104					
115	JHARS_GR	63	85			ROUTER	IEC104					
116	JKPPR_GR	10	5			TS	IEC101					
117	BOLAN_GR	17	39			ROUTER	IEC104					
118	JUNAG_GR	42	84			ROUTER	IEC104					
119	KHARI_GR	42	89			ROUTER	IEC104					
120	SORO__GR	52	103			ROUTER	IEC104					
121	RKHOL_GR	45	94			ROUTER	IEC104					
122	SALIP_GR	55	109			ROUTER	IEC104					
123	SONEP_GR	52	107			ROUTER	IEC104					
124	POLAS_GR	79	168			ROUTER	IEC104					
125	SAINT_GR	40	87			ROUTER	IEC104					
126	ANAND_GR	58	93			ROUTER	IEC104					

127	BALUG_GR	58	17			ROUTER	IEC104					
128	BARPA_GR	42	88			ROUTER	IEC104					
129	BASTA_GR	49	76			ROUTER	IEC104					
130	BRAJA_GR	104	149			TS	IEC101					
131	CHNDI_GR	58	115			ROUTER	IEC104					
132	CHEND_GR	67	145			ROUTER	IEC104					
133	DIGAP_GR	64	128			ROUTER	IEC104					
134	JAGAT_GR	59	118			ROUTER	IEC104					
135	JAJTW_GR	56	119			ROUTER	IEC104					
136	JALES_GR	61	110			ROUTER	IEC104					
137	KARAN_GR	52	82			ROUTER	IEC104					
138	KESUR_GR	49	62			ROUTER	IEC104					
139	NIMPA_GR	52	103			ROUTER	IEC104					
140	NAUPA_GR	59	116			TS	IEC101					
141	PARLA_GR	43	83			ROUTER	IEC104					
142	PATNA_GR	56	113			ROUTER	IEC104					
143	PATAM_GR	50	98			ROUTER	IEC104					
144	PHULB_GR	50	98			ROUTER	IEC104					
145	PHULN_GR	51	106			ROUTER	IEC104					

146	TENTU_GR	47	96			ROUTER	IEC104					
147	SUNDA_GR	65	123			ROUTER	IEC104					
148	KJHAR_GR	59	77			ROUTER	IEC104					
149	MOHAN_GR	37	56			ROUTER	IEC104					
150	KALAR_GR	43	89			ROUTER	IEC104					
151	ARGUL_GR	57	58			TS	IEC101					
152	SAMUK_GR	43	54			TS	IEC101					
153	BANKI_GR	28	30			ROUTER	IEC104					
154	TELKO_GR	30	39			ROUTER	IEC104					
155	JSWCE_GR	22	28			ROUTER	IEC104					
156	LAPAN_GR	114	207			ROUTER	IEC104					
157	BAMNI_GR	7	6			ROUTER	IEC104					
158	SMC__GR	14	23			TS	IEC101					
159	TATA__GR	18	17			TS	IEC101					
160	OISL__GR	14	18			TS	IEC101					
161	BRPL2_GR	12	18			TS	IEC101					
162	ROHIT_GR	11	7			TS	IEC101					
163	BALOY_GR	27	23			ROUTER	IEC104					
164	BTYRE_GR	25	10			ROUTER	IEC104					

165	MESCO_GR	17	15			TS	IEC101					
166	FAP___GR	6	4			ROUTER	IEC104					
167	JSTEL_GR	9	14			ROUTER	IEC104					
168	BCMOH_GR	21	21			TS	IEC101					
169	IOCL__GR	24	13			TS	IEC101					
170	PMU__GR	116	36			ROUTER	IEC104					
171	IFFCO_GR	14	11			TS	IEC101					
172	MSPJD_GR	9	6			TS	IEC101					
173	CHNDP_GR	35	34			ROUTER	IEC104					
174	ESAR2_GR	13	7			TS	IEC101					
175	KAROD_GR	61	110			ROUTER	IEC104					
176	DHMRA_GR	65	70			TS	IEC101					
177	DAKSH_GR	23	11			ROUTER	IEC104					
178	BARBI_GR	39	54			TS	IEC101					
179	IB400_GR	36	137			ROUTER	IEC104					
180	UNIT8_GR	52	46			ROUTER	IEC104					
181	KONAR_GR	52	58			ROUTER	IEC104					
182	SHREE_GR	6	7			ROUTER	IEC104					
183	EMAMI_GR	29	17			ROUTER	IEC104					

184	TSALY_GR	17	23			TS	IEC101						
185	MANCH_GR	58	62			ROUTER	IEC104						
186	NALDM_GR	59	58			ROUTER	IEC104						
187	KALUG_GR	22	39			TS	IEC101						
188	KHUNT_GR	40	58			ROUTER	IEC104						
189	BHAWA_GR	63	66			ROUTER	IEC104						
190	NARSG_GR	55	84			ROUTER	IEC104						
191	MSAL__GR	58	82			ROUTER	IEC104						
192	GODA__GR	79	97			ROUTER	IEC104						
193	RAMCO_GR	19	21			ROUTER	IEC104						
194	PRATP_GR	91	116			ROUTER	IEC104						
195	GUDAY_GR	42	66			ROUTER	IEC104						
196	BPPPL_GR	16	7			ROUTER	IEC104						
197	MAHI1_GR	10	2			ROUTER	IEC104						
198	IBC__GR	7	1			ROUTER	IEC104						
199	JYOTI_GR	7	1			ROUTER	IEC104						
217	AFTAB_GR	7	1			ROUTER	IEC104						
218	JAYIR_GR	7	1			ROUTER	IEC104						
219	MOHAB_GR	7	1			ROUTER	IEC104						

220	VIVCY_GR	7	1			ROUTER	IEC104					
221	SNMOH_GR	7	1			ROUTER	IEC104					
222	RAJRA_GR	7	1			ROUTER	IEC104					
223	MGMSO__GR	7	1			ROUTER	IEC104					
224	ABCUS_GR	7	1			ROUTER	IEC104					
225	MAHI2_GR	10	2			ROUTER	IEC104					
226	ACME__GR	33	28			ROUTER	IEC104					

D. Sikkim

S. No.	RTU Location /Station	Number Of Analogs data point s in the RTU	Number Of Digital data points in the RTU	Make	Existing Control Centre name to which RTU reports presently (i.e. Sub-LDC or SLDC or RLDC)	Communication Interface at RTU side	Existing Interface at Control Center		Proposed Interface at Control Center		Proposed Interface at Backup Control Center	
							Port at CFE	No. of Channels	Port at CFE	No. of Channels	Port at CFE	No. of Channels
1	LLHP 66	25	56	CALLISTO	SLDC	ADSS	ICE 104	1			ICE 104	1
2	TADONG 66	25	19	C264	SLDC	ADSS	ICE 104	1			ICE 104	1
3	BULBULAY66	25	11	C264 C	SLDC	ADSS	ICE 104	1			ICE 104	1
4	SICHEY 66	25	13	C264	SLDC	ADSS	ICE 104	1			ICE 104	1
5	PHODONG 66	25	11	C264	SLDC	ADSS	ICE 104	1			ICE 104	1
6	MANGAN 66	25	11	C264	SLDC	ADSS	ICE 104	1			ICE 104	1
7	GYALSHING 66	25	62	CALLISTO	SLDC	ADSS	ICE 104	1			ICE 104	1
8	MACLEOIDS 66	13	3	CALLISTO	SLDC	ADSS	ICE 104	1			ICE 104	1
9	MELLI 132 & 66	54	135	CALLISTO	SLDC	ADSS	ICE 104	1	ICE 104	1	ICE 104	1
10	MAMRING 66	14	33	CALLISTO	SLDC	OPGW			ICE 104	1	ICE 104	1
11	NAMCHI 66	21	49	CALLISTO					ICE 104	1	ICE 104	1
12	PELLING 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1

13	SAGBARI 66				SLDC	OPGW(Under progress)			ICE 104	1	ICE 104	1
14	PAKYONG 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
15	RONGLI 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
16	RHENOCK 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
17	TOPAKHANI 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
18	MEYONG 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
19	SORENG 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
20	SOMBAREY 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
21	ROTHAK 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
22	LACHUNG 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
23	RAVANGLA 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
24	RABOM HEP 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
25	JORETHANG 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1
26	MALTIN 66				SLDC	OPGW (Under progress)			ICE 104	1	ICE 104	1

27	PERBING 66				SLDC	OPGW(Under progress)			ICE 104	1	ICE 104	1
28	OLD NAMCHI 66				SLDC	OPGW(Under progress)			ICE 104	1	ICE 104	1
29	SHERATHANG 66				SLDC	OPGW(Under progress)			ICE 104	1	ICE 104	1
30	MARCHAK 66				SLDC	OPGW(Under progress)			ICE 104	1	ICE 104	1
31	YANGANG 66				SLDC	OPGW(Under progress)			ICE 104	1	ICE 104	1
32	KHAMDONG 66				SLDC	OPGW(Under progress)			ICE 104	1	ICE 104	1

E. BSPTCL

S.No.	RTU Location/Station	Number of Analog Data Points in the RTU	Number of Digital Data Points in the RTU	Make	QUANTITY OF RTU	Existing Control Centre name to which RTU reports presently (i.e Sub-LDC or SLDC or RLDC)	Communication Interface at RTU side	Existing Interface at RTU side		Proposed Interface at Control Center		Proposed Interface at Backup Control Center		Existing RTU or New RTU
								Port at CFE	No. of Channels	Port at CFE	No. of Channels	Port at CFE	No. of Channels	
1	ARARIA	81	161	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
2	ARERAJ	73	150	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
3	ARRAH	138	297	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
4	AURANGABAD	77	181	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
5	BAISI	38	107	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
6	BAKHARI	69	144	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
7	BALLIA	72	136	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
8	BANJARI	54	132	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
9	BANKA	182	367	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	PDH	RS 232	2	RS 232	4	RS 232	4	Existing
10	BANKA NEW	101	194	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
11	BANMANKHI	73	150	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
12	BARH	128	223	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
13	BARIPAHARI	63	155	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
14	BARSOI	77	155	SYNERGY	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
15	BEGUSARAI	219	608	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
16	BELAGANJ	45	116	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
17	BELSAND	51	101	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
18	BENIPATTI	76	139	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
19	BENIPUR	88	196	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing

20	BETIAH	100	235	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
21	BHAGALPUR NEW (JAGDISHPUR)	81	194	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
22	BHABHUA	81	161	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
23	BIHARSHARIF	176	452	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
24	BIHTA	149	271	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
25	BIHTA NEW	132	324	GE	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
26	BIKRAMGNJ	135	250	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
27	BODHGAYA	161	410	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
28	BTPS_NEW	68	169	SAS-SIEMENS	1	SLDC & ERLDC	PDH	RS 232	1	RS 232	2	RS 232	2	Existing
29	BTPS_OLD	76	186	SAS-SIEMENS	1	SLDC & ERLDC	PDH	RS 232	1	RS 232	2	RS 232	2	Existing
30	BUXAR	146	306	CHEMTROLS	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
31	CHAKIA	58	96	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
32	CHANDAUTI	66	189	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
33	CHAPRA	66	178	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
34	DALSINGSARAI	122	223	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
35	DARBHANGA132	72	170	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
36	DARBHANGA220	65	201	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
37	DALMIA	5	14	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing

36	DARBHANGA220	65	201	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
37	DALMIA	5	14	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
38	DEHRI	243	562	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
39	DHAKA	69	215	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
40	DHAMDAHA	80	150	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
41	DHANAHA	72	167	CHEMTROLS	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
42	DIGHA	155	243	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	PLCC	RS 232	2	RS 232	4	RS 232	4	Existing
43	DINARA (KOCHAS)	115	216	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	PLCC	RS 232	2	RS 232	4	RS 232	4	Existing
44	DUMRAON	162	284	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
45	EKANGASARAI	111	230	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
46	EKMA	24	46	CHEMTROLS	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
47	FATUHA	405	878	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
48	FORBESGANJ	270	540	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
49	GAIGHAT	135	240	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
50	GANGWARA	59	143	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
51	GOH	126	251	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
52	GOPALGANJ	105	277	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
53	HAJIPUR	116	255	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
54	HAJIPUR 220KV	68	193	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
55	HARNAUT	119	216	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
56	HATHIDAH	59	181	CHEMTROLS	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
57	HATHUA	89	173	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
58	HULASGANJ	47	113	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
59	IMAMGUNJ	47	123	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
60	JAGDISPUR	117	223	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
61	JAHANABAD	97	200	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
62	JAI NAGAR	61	157	CHEMTROLS	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
63	JAKKANPUR	127	227	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
64	JAMALPUR	89	171	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
65	JAMUI	81	194	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing

66	JAMUI NEW	81	163	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing

67	JANDAHA	130	243	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
68	JHANJHARPUR	76	142	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
69	KAHALGAON	154	297	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
70	KARBIGAHIYA	85	207	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
71	KARMANASA	149	338	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
72	KARMANASA NEW	238	444	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
73	KARPI (ATAULA)	55	132	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
74	KATAIYA	142	162	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	PLCC	RS 232	2	RS 232	4	RS 232	4	Existing
75	KATIHAR	101	225	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
76	KATRA	135	257	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
77	KBUNL-STAGE 1	77	208	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
78	KHAGARIA	57	149	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
79	KHAGARIA NEW	154	446	SAS	1	SLDC & ERLDC	PLCC	RS 232	2	RS 232	4	RS 232	4	Existing
80	KHAGAUL	243	520	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
81	KISHANGANJ	155	169	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
82	KISHANGANJ NEW	135	439	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
83	KUDRA	123	230	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	PLCC	RS 232	2	RS 232	4	RS 232	4	Existing
84	KUSHESWAR ASTHAN	122	250	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
85	LAKHISARAI	96	234	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
86	LAUKAHI	108	224	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
87	MADHEPURA	205	500	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
88	MADHUBANI	101	230	CHEMTROLS & SYNERGY	1	SLDC & ERLDC	PDH	RS 232	1	RS 232	2	RS 232	2	Existing
89	MAHANAR	77	155	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
90	MAHARAJGANJ	68	131	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
91	MANIHARI	73	150	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
92	MANJHAUL	63	126	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
93	MASAURHI	113	216	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing

94	MASHRAKH	128	236	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
95	MITHAPUR	135	234	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
96	MOHANIA	101	176	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
97	MOTIHARI	203	389	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
98	MOTIPUR	135	956	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
99	MUSHAHARI	113	508	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
100	MUZAFFARPUR	100	225	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
101	NABINAGAR	14	54	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
102	NALANDA	162	177	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
103	NARKTIYAGANJ	73	203	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
104	NAUGACHIA	66	180	CHEMTROLS	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
105	NAWADA	132	284	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
106	NIRMALI	72	140	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
107	PAKRIDAYAL	51	101	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
108	PANDAUL	81	184	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
109	PHULPARAS	123	251	CHEMTROLS & SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
110	PIRO	81	154	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
111	PUPARI	51	101	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
112	PURNIA	97	242	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
113	PUSAULI	134	328	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
114	RAFIGANJ	84	186	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
115	RAILWAY TSS	281	70	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
116	RAGHOPUR	90	185	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
117	RAGHUNATHPUR	107	198	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
118	RAJGIR	39	123	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
119	RAMGARH	107	215	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
120	RAMNAGAR	72	177	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
121	RAXAUL	63	139	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
122	ROSERA	59	119	SYNERGY	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
123	RUNNISADPUR	63	151	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
124	SABOUR	104	230	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
125	SAHARSA	331	446	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing

126	SAMASTIPUR NEW	95	392	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
127	SAMASTPUR	97	236	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing

128	SASARAM	119	243	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
129	SHAHPURPATORI	77	151	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
130	SHEIKPURA	176	344	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
131	SHEOHAR	68	131	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
132	SHERGAHTI	115	189	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
133	SHETALPUR	76	181	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
134	SIMRI BAKHTIYARPUR	73	150	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
135	SIPARA	216	441	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	PDH	RS 232	2	RS 232	4	RS 232	4	Existing
136	SITAMARHI	85	205	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
137	SIWAN	171	338	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
138	SKMCH	73	178	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
139	SONEBARSA	128	257	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
140	SONENAGAR	123	304	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
141	SONENAGAR NEW	81	414	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
142	SULTANGANJ	128	328	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
143	SUPAUL	69	189	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
144	TARAPUR	73	150	SYNERGY	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
145	TEGHARA	63	126	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
146	TEHTA	55	138	CHEMTROLS	1	SLDC & ERLDC	PDH	RS 232	1	RS 232	2	RS 232	2	Existing
147	TEKARI	51	123	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
148	TRIVENIGANJ	73	150	SYNERGY	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
149	UDAKISANGANJ	111	223	CHEMTROLS & SYNERGY	2	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
150	ULTRATECH	135	81	CHEMTROLS	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
151	VAISHALI	74	171	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
152	VALMIKINAGAR	61	109	CHEMTROLS	1	SLDC & ERLDC	PLCC	RS 232	1	RS 232	2	RS 232	2	Existing
153	WARSALIGANJ	101	196	SYNERGY	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
154	WAZIRGANJ	51	123	CHEMTROLS	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
155	BIHTA NEW	14	14	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
156	CHHAPRA NEW	99	171	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
157	DUMRAON NEW	134	289	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
158	GAYA NEW	77	381	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
159	GORADI NEW	165	373	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
160	HAJIPUR NEW	28	72	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing

161	JAMALPUR NEW	163	347	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
162	KHAGAUL NEW	14	14	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing

163	MOKAMA NEW	135	270	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
164	NAWADA NEW	43	248	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
165	SHEIKHPURA NEW	72	180	SAS	1	SLDC & ERLDC	OPGW	Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
166	ASTHAWAN	189	459	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
167	BAGHA	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
168	BAKHTIYARPUR	270	608	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
169	BARACHATTI	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
170	BARARI	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
171	BHORE	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
172	BOARD COLONY	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
173	DAUDNAGANR	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
174	DIGHA NEW	189	459	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
175	GORAUL	189	459	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
176	HARINAGAR	81	189	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
177	KERPA	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
178	KORHA	189	459	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
179	LAURIYA	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
180	MURLIGANJ	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
181	NAVINAGAR	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
182	PALASI	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
183	PALIGANI	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
184	RAXAUL NEW	189	459	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
185	SUGAULI	81	189	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
186	TAJPUR	81	189	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
187	ACME SOLAR	27	11	RTU	2	SLDC & ERLDC		Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
188	AVANTIKA SOLAR	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
189	AVAADA SOLAR	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
190	AZURE SOLAR	14	5	RTU	1	SLDC & ERLDC	OPGW	Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
191	SHERGHATI SOLAR	27	11	RTU	2	SLDC & ERLDC		Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing
192	SAVAKALA SOLAR	14	5	RTU	1	SLDC & ERLDC		RS 232	1	RS 232	2	RS 232	2	Existing
193	GLATT SOLAR	27	11	RTU	2	SLDC & ERLDC		Ethernet port	2	Ethernet port	4	Ethernet port	4	Existing

194	RESPONSE SOLAR	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
195	UDIPTA SOLAR	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
196	SWADESHI SUGAR	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
197	DISTILLERS BIOFUEL	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
198	TIRUPATI SUGAR	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing

199	HARINAGAR SUGAR MILL	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
200	BHARAT SUGAR PLANT	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
201	HASANPUR SUGAR MILL	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
202	RIGA SUGAR MILL	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
203	LAURIYA HPCL BIOFUEL	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
204	HPCL BIOFUEL, SUGAULI	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
205	SIDDHASHRAM SUGAR MILL	14	5	RTU	1	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
206	HYDROPOWER PLANT	108	270	RTU	5	SLDC & ERLDC		Ethernet port	1	Ethernet port	2	Ethernet port	2	Existing
		20069	43693		258				274		548		548	

F. JUSNL

S. No.	RTU Location/Station	Number Of Analogs data points in the RTU	Number Of Digital data points in the RTU	Make	Existing Control Centre name to which RTU reports presently (i.e. Sub-LDC or SLDC or RLDC)	Communication Interface at RTU side	Existing Interface at Control Center		Proposed Interface at Main Control Center		Proposed Interface at Back-up Control Center	
							Port at CFE	No. of Channels	Port at CFE	No. of Channels	Port at CFE	No. of Channels
1	Hatia-I	122	248	Synergy	SLDC, Kusai	Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
2	Hatia-II	106	242	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
3	Namkum	86	197	Chemtrols		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
4	Kanke	70	160	Chemtrols		Serial Interface	IEC 101	1	IEC 104, Port	2	IEC 104, Port	2
5	Gumla	54	128	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 104, Port	2
6	Khunti	80	150	ABB		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
7	Tamar	105	170	ZIV (SAS)		Serial Interface	IEC 101	1	IEC 104, Port	2	IEC 104, Port	2
8	Loherdaga	83	182	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
9	Simdega	48	130	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2

10	Sikidiri	73	147	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
11	Kamdara	88	175	Chemtrols		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
12	Ranchi GIS (Smart City)	105	172	SAS		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
13	Pakur	67	156	Chemtrols		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
14	Maharo	91	210	Chemtrols		Serial Interface	IEC 101	1	IEC 101	2	IEC 104, Port	2
15	Sahebganj	67	156	Chemtrols		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
16	Rajmahal	90	150	SAS (Amaraza)		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
17	Deoghar	113	198	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 104, Port	2
18	Madhupur	80	130	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
19	Jamua	88	145	SAS		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
20	Jamtara	92	177	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
21	Lalmatia	95	194	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
22	Godda	131	242	SAS (ZIV)		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
23	Madanpur	82	183	SAS (Schnieder)		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
24	Jasidih	105	230	SAS (ZIV)		Serial Interface	IEC 101	1	IEC 101	2	IEC 104, Port	2
25	Giridih	138	354	SAS (Siemens)		Serial Interface	IEC 101	1	IEC 101		IEC 104,	

											Port	
26	Manoharpur	90	150	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
27	Chandil	100	180	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
28	Noamundi	40	89	Chemtrols		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
29	Rajkharsawan	90	158	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
30	Jadugoda	86	164	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
31	Dalbhumgarh	63	174	Chemtrols		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
32	Chaibasa 220 KV	116	316	SAS (Schnieder)		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
33	Manique	62	123	Chemtrols		Serial Interface	IEC 101	1	IEC 101	2	IEC 104, Port	2
34	Golmuri	62	152	Chemtrols		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
35	Adityapur	101	288	Chemtrols		Serial Interface	IEC 101	1	IEC 101	2	IEC 104, Port	2
36	Kendposi	79	160	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
37	Goelkera	67	119	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
38	Mango	70	117	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
39	Bahragoda	76	155	SAS		Serial Interface	IEC 101	1	IEC 101	2	IEC 104, Port	2
40	Ramchandrapur 220 KV	93	103	Synergy		Ethernet	IEC 104, Port	1	IEC 104,	2	IEC 104,	2

									Port		Port	
41	Ramchandrapur 132 KV	53	77	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 104, Port	2
42	Chakradharpur	40	75	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
43	Garhwa 132 KV	95	196	Synergy		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
44	Japla	67	156	Chemtrols		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
45	Daltonganj	72	161	Chemtrols		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
46	Garhwa 220KV	148	306	SAS		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
47	Latehar	69	157	Chemtrols		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
48	Tenughat	128	296	Synergy		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
49	Patratu 400 KV	97	217	SAS (Siemens)		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
50	Govindpur	120	317	SAS (CGL)		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
51	Saria	92	143	SAS		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
52	Nagaruntari	42	80	RTU (ABB)		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
53	Chatra	113	236	SAS (ZIV)		Serial Interface	IEC 101	1	IEC 101	2	IEC 101	2
54	Latehar New (400 KV)	120	250	(SAS) GE		Ethernet	IEC 104, Port	1	IEC 104, Port	2	IEC 104, Port	2
55	Chitra			NA					IEC 104, Port	2	IEC 104, Port	2
56	Chaibasa 132 KV			NA					IEC 104, Port	2	IEC 104, Port	2

G. ERLDC

	RTU Location/Station	Number Of Analogs data points in the RTU	Number Of Digital data points in the RTU	Make	Existing Control Centre name to which RTU reports presently (i.e. Sub-LDC or SLDC or RLDC)	Communication Interface at RTU side	Existing Interface at Control Center		Proposed Interface at Control Center		Proposed Interface at Backup Control Center	
1	Bheramara HVDC	117	258	Siemens SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
2	Jamshedpur	60	200	Alstom S900 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
3	Biharsharif	90	250	Alstom S900 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
4	Purnea 220	40	110	Alstom C264 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
5	Purnea New	80	245	Alstom S900 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
6	Sasaram 400	90	250	Alstom S900 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
7	Muzaffarpur	80	250	Alstom S900 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
8	Arrah 220	40	100	Nelco, RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2

9	New Sasaram 765	40	120	Alstom SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
10	Gaya	120	400	Siemens SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
11	Banka	50	200	Alstom SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
12	Lakhisarai	50	200	Alstom SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
13	Chaibasa	60	250	Siemens SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
14	New Ranchi	110	370	Siemens SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
15	Birpara AIS	40	110	Alstom C264 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
16	Dalkhola	30	80	Alstom C264 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
17	Durgapur	80	250	Alstom S900 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
18	Gangtok	20	40	Alstom C264 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
19	Maithan	90	260	Alstom S900 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
20	Malda	60	160	Alstom C264 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
21	Rangpo	100	290	SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
22	Siliguri 220	50	120	Alstom C264 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
23	Binaguri	100	340	Alstom S900 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
24	Subhasgram	60	220	Alstom C264 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2

25	Angul	90	400	SAS-SIEMENS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
26	Bolangir	40	150	SAS-SIEMENS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
27	Keonjhor	90	250	SAS-SIEMENS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
28	Talcher HVDC	95	150	SAS-SIEMENS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
29	Jharsuguda SAS	150	610	SAS-SIEMENS	ERLDC	Serial Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
30	Indravati	30	90	AlstomRTU-C264	ERLDC	Ethernet Interface	IEC 101	2	IEC 101	2	IEC 101	2
31	Jeypore	80	220	AlstomRTU-S900	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
32	Kalabadia	70	220	AlstomRTU-C264	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
33	Rengali	40	110	AlstomRTU-C264	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
34	Rourkella	80	220	AlstomRTU-S900	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
35	Kahalgaon STPS	130	320	GE SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
37	Lalmatia	30	80	Alstom S900 RTU	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
38	Nabinagar	60	240	SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
39	Rangit HEP	60	210	GE SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
40	GMR	40	170	SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
41	Chuzachen	25	40	Alstom SAS	ERLDC	Serial Interface	IEC	2	IEC	2	IEC 101	2

	HEP						101		101			
42	JITPL	35	120	SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
43	Teesta 3 HEP	45	210	Andriz Hydro SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
44	Dikchu HEP	38	195	SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
45	Jorethang	25	75	SAS	ERLDC	Serial Interface	IEC 101	2	IEC 101	2	IEC 101	2
46	Ranchi	80	250	Siemens SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
47	Kishanganj	105	270	Siemens SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
48	Daltonganj	115	520	GE SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
49	Chandauti	155	520		ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
50	Baharampur	35	90	Siemens SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
52	Barh STPS	90	380	SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
53	NPGC	60	290		ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
54	KBUNL Stage 2	60	210		ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
55	Darliparli STPS	80	480		ERLDC	Ethernet Interface	IEC	2	IEC	2	IEC 104	2

							104 , Port		104 , Port		, Port	
56	Teesta V	25 (1 nof Intergral Value for rain fall)	70	GE SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
57	Maithan Right Bank	50	210	ABB SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
58	Patna	90	320	Alstom SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
59	Chandwa	50	150	ABB SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
60	Alipurduar	110	450	ABB SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
61	Birpara GIS	20	50		ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
62	Melli New	40	90	SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
63	Rajarhat	50	240	Siemens SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
64	Pandiabili	55	190	SAS-SIEMENS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
66	New Farakka	100	260	GE SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
67	Darbhanga	75	330	Siemens SAS	ERLDC	Ethernet Interface	IEC	2	IEC	2	IEC 104	2

							104 , Port		104 , Port		, Port	
68	APNRL	30	90	ABB SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
69	Talcher STPS	100	320	Alstom S900 RTU	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
70	Saharsa	115	340	Siemens SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
71	Sitamarhi	80	395	Siemens SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
72	Dhanbad	60	200	Siemens SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
73	North karanpura TPS	70	230	--	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
74	TASHIDING	20	76	GE SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2
75	MOTIHARI	63	346	Siemens SAS	ERLDC	Ethernet Interface	IEC 104 , Port	2	IEC 104 , Port	2	IEC 104 , Port	2

Vol. II, Part-A

Appendix - B

Interoperability Profile of IEC 60870-5-101 and IEC60870-5-104

Typical Interoperability Profile of IEC 60870-5-101 protocol

This companion standard presents sets of parameters and alternatives from which subsets have to be selected to implement particular telecontrol systems. Certain parameter values, such as the number of octets in the COMMON ADDRESS of ASDUs represent mutually exclusive alternatives. This means that only one value of the defined parameters is admitted per system. Other parameters, such as the listed set of different process information in command and in monitor direction allow the specification of the complete set or subsets, as appropriate for given applications. This clause summarizes the parameters of the previous clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment stemming from different manufacturersit is necessary that all partners agree on the selected parameters.

The selected parameters should be marked in the white boxes as follows:

□	Function of ASDU is not used
■	Function or ASDU is used as standardized (default)

Note : In addition, the full specification of a system may require individual selection ofcertain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values

1.1 SYSTEM or DEVICE

(System-specific parameter, indicate the definition of a system or a device by marking one of the following with an ' X'

☐ System definition

☐ Controlling station definition (master)

■ Controlled station definition (Slave)

1.2 NETWORK CONFIGURATION

(Network-specific parameter, all configurations that are used are to be marked with ' ☒ ')

■ Point-to-point

■ Multiple point-to-point

■ Multipoint-party line

□ Multipoint-star

1.3 PHYSICAL LAYER (Network-specific parameter)

Transmission speed (control direction) :

Unbalanced interchange circuit V.24/V.28 Standard		*Unbalanced interchange circuit V.24/V.28 Recommended if >1 200 bit/s*		*Balanced interchange circuit X.24/X.27*	
☐	100 bit/s	☐	2 400 bit/s	☐	2 400 bit/s
■	200 bit/s	☐	4 800 bit/s	☐	4 800 bit/s
■	300 bit/s	☐	9 600 bit/s	☐	9 600 bit/s
■	600 bit/s			☐	19 200 bit/s
■	1200 bit/s			☐	38 400 bit/s
(for unbalanced transmission only				☐	56 000 bit/s
				☐	64 000 bit/s

Transmission speed (monitor direction) :

Unbalanced interchange circuit V.24/V.28 Standard		*Unbalanced interchange circuit V.24/V.28 Recommended if >1 200 bits/s*		*Balanced interchange circuit X.24/X.27*	
☐	100 bit/s	☐	2 400 bit/s	☐	2 400 bit/s
■	200 bit/s	☐	4 800 bit/s	☐	4 800 bit/s
■	300 bit/s	☐	9 600 bit/s	☐	9 600 bit/s
■	600 bit/s			☐	19 200 bit/s
■	1 200 bit/s			☐	38 400 bit/s
(for unbalanced transmission only)				☐	56 000 bit/s
				☐	64 000 bit/s

1.4 LINK LAYER *(Network-specific parameter)*

Frame format FT 1.2, single character 1 and the fixed time out interval are used exclusively in this companion standard.

Link transmission procedure

□ Balanced transmission

■ Unbalanced transmission

Address field of the link

□ Not present (balanced transmission only)

■ One octet

☐ Two octets

☐ Structured

■ Unstructured

Frame length

255 Maximum length L (number of octets)

1.5 APPLICATION LAYER

Transmission mode for application data

Mode 1 (Least significant octet first), as defined in clause 4.10 of IEC 870-5-4, is used exclusively in this companion standard.

Common address of ASDU
(system-specific parameter)

■ One octet □ Two octets

Information object address
(system-specific parameter)

☐ One octet □ Structured

■ Two octets ■ Unstructured

☐ Three octets

Cause of transmission
(system-specific parameter)

■ One octet □ Two octets (with originator address)

Selection of standard ASDUs
(station-specific parameter)

■ <1> := Single-point information M_SP_NA_1

■ <2> := Single-point information with time tag M_SP_TA_1

☐ <3> := Double-point information M_DP_NA_1

☐ <4> := Double-point information with time tag M_DP_TA_1

☐ <5> := Step position information M_ST_NA_1

☐ <6> := Step position information with time tag M_ST_TA_1

■ <7> := Bit string of 32 bit M_BO_NA_1

☐ <8> := Bit string of 32 bit with time tag M_BO_TA_1

■ <9> := Measured value, normalized value M_ME_NA_1

☐ <10> := Measured value, normalized value with time tag M_ME_TA_1

■ <11> := Measured value, scaled value M_ME_NB_1

☐ <12> := Measured value,a scaled value with time tag M_ME_TB_1

☐ <13> := Measured value, short floating point value M_ME_NC_1

☐ <14> := Measured value, short floating point value with time tag M_ME_TC_1

■ <15> := Integrated totals M_IT_NA_1

☐ <16> := Integrated totals with time tag M_IT_TA_1

☐ <17> := Event of protection equipment with time tag M_EP_TA_1

☐ <18> := Packed start events of protection equipment with time tag

M_EP_TB_1

☐ <19> := Packed output circuit information of protection equipment with time tag
M_EP_TC_1

☐ <20> := Packed single-point information with status change detection
M_PS_NA_1

☐ <21> := Measured value, normalized value without quality descriptor M_ME_ND_1

Process information in control direction
(station-specific parameter)

■ <45> := Single command
C_SC_NA_1

■ <46> := Double command
C_DC_NA_1

☐ <47> := Regulating step command C_RC_NA_1

■ <48> := Set point command, normalized value
C_SE_NA_1
(required only for analog output command)*

■ <49> := Set point command, scaled value
C_SE_NB_1

☐ <50> := Set point command, short floating point value C_SE_NC_1

☐ <51> := Bit string of 32 bit
C_BO_NA_1

System information in monitor direction
(station-specific parameter)

■ <70> := End of initialization
M_EI_NA_1

System information in control direction
(station-specific parameter)

■ <100> := Interrogation command C_IC_NA_1

■ <101> := Counter interrogation command C_CI_NA_1

□ <102> := Read command C_RD_NA_1

■ <103> := Clock synchronization command C_CS_NA_1 (optional, if GPS is used for time synch. of the RTU)*

□ <104> := Test command C_TS_NA_1

☐ <105> := Reset process command C_RP_NA_1

■ <106> := Delay acquisition command C_CD_NA_1

(optional, if GPS is used for time synch. of the RTU)*

Parameter in control direction
(station-specific parameter)

☐ <110> := Parameter of measured value, normalized value P_ME_NA_1

☐ <111> := Parameter of measured value, scaled value P_ME_NB_1

☐ <112> := Parameter of measured value, short floating point value P_ME_NC_1

☐ <113> := Parameter activation P_AC_NA_1

File transfer *(for downloading of database from RLDC, may not be required)* *
(station-specific parameter)

■ <120> := File ready F_FR_NA_1

- <121> := Section ready F_SR_NA_1
- <122> := Call directory, select file, call file, callsection F_SC_NA_1
- <123> := Last section, lastsegment F_LS_NA_1
- <124> := Ack file, ack section F_AF_NA_1
- <125> := Segment F_SG_NA_1
- <126> := Directory F_DR_TA_1

BASIC APPLICATION FUNCTIONS

Station initialization
(station-specific parameter)

- Remote initialization

General interrogation
(system or station-specific parameter)

■ Global		
■ Group 1	■ Group 7	■ Group 13
■ Group 2	■ Group 8	■ Group 14
■ Group 3	■ Group 9	■ Group 15
■ Group 4	■ Group 10	■ Group 16
■ Group 5	■ Group 11	
■ Group 6	■ Group 12	

Addresses per group have to be defined

Clock synchronization
(station-specific parameter)

- Clock synchronization (optional, if GPS is used for time synch. of the RTU)*

Command transmission (Required only when control command is envisaged)*(object-specific parameter)

■ Direct command transmission	■ Select and execute command
■ Direct set point command transmission	■ Select and execute set point

☐ C_SE ACTTERM used

■ No additional definition
□ Short pulse duration (duration determined by a system parameter in the outstation)
□ Long pulse duration (duration determined by a system parameter in the outstation)
□ Persistent output

Transmission of integrated totals
(station or object-specific parameter)

■ Counter request
■ Counter freeze without reset
■ Counter freeze with reset
☐ Counter reset

□ General request counter
□ Request counter group 1
□ Request counter group 2
□ Request counter group 3
□ Request counter group 4

Addresses per group have to be defined

Parameter loading
(object-specific parameter)

☐ Threshold value
☐ Smoothing factor
☐ Low limit for transmission of measured value
☐ High limit for transmission of measured value

Parameter activation
(object-specific parameter)

☐ Act/Deact of persistent cyclic or periodic transmission of the addressed object

File transfer
(station-specific parameter)

■ File transfer in monitor direction
■ File transfer in control direction ***(For downloading of database from RLDC, May not be required)****

Additional Information on IEC 60870-5-101

A. Telemetered Data and ASDU mapping

The following table explains the type of the telemetered data and corresponding ASDUs used to transmit this data as per IEC 60870-5-101 protocol.

Type of power system Data	**Data Unit type as per IEC**	**Descriptio nas per IEC**	**Data polling method**	**Interro gation group**	**Transmit ted after Class-X request**	**Info Obj. Addre ss range**
Analog inputs (P,Q, V, f)	ASDU-9	Measured value normalize dvalue	By periodic Group scan	Group-2	Class 2	2001-3000
Digital inputs – Single status (Circuit breakers, Isolators, Protection signals)	ASDU-1	Single point informati on	By exception (spontaneous) and on periodic Group scan	Group-1	Class 1 after exception, Class 2 after Group 1 scan	1-1000
	ASDU- 2 (for SOE)	Single point information with time tag	By exception (spontaneous)		Class 1 after exceptio nn	1001-2000
Pulse accumulators	ASDU-15	Integrate dtotals	By periodic counter interrogation	Group-1 (counter interrogat etion)	Class 2	4001-5000
Analog Outputs (Setpoint)	ASDU-48	Set point command Normalize dvalue				5001-6000
Digital Control command (CB Trip/Close)	ASDU 45	Single comman d				3001-4000

B. Data polling method

1. The RTU shall respond to the Master stations request for the at least the following commands as per the protocol:

   - Status of Link
   - Reset of Link
   - Delay acquisition command
   - Clock synchronization command
   - General interrogation command
   - Interrogation of Scan group 1 command (all status data)
   - Interrogation of Scan group 2 command (all analog data)
   - Class 1/2 data polling

If supervisory control commands are envisaged, then SBO procedure is to be used.

2. Normal data polling is by Scan groups
3. All digital inputs are assigned to Scan group-1 and all Analog values are assigned to Scan group-2
4. Analog values are acquired periodically by using the Scan group-2 polling. This periodicity is ranging from 10-15 seconds based on the quantity of analogs and the communication channel bandwidth.
5. Digital input state changes are reported spontaneously by RTU as class 1 data and a integrity scan is performed for all the digital inputs using Scan group-1 at every 10 minutes interval.
6. Double bit digital status data are to be sent as two single-point information from the RTU.

Introduction to the IEC 60870-5-104 standard

The remote control of substations or power plants, using IEC 60870 5-104 standard, allows the utility to control locations separated long distances from a centralized control room optimizing the use of resources for that task.

The definition of standardized remote control protocols makes it possible to integrate systems automated by different vendors with the utility control centre. This allows controlling the system without the need of protocol converters or adaptations.

When the communication options were limited due to the bandwidth available, the remote control protocols used serial communication through radio links or the telephone networks in most cases though private networks.

Within these capabilities, IEC defined the remote control protocol called IEC 60870-5-101. This standard includes a set of messages called ASDU and a set of application functions available to monitor and control remote stations through the serial channels available at that time.

The arrival of TCP/IP connectivity channels to the remote stations by the use of dedicated optical fibers, digital radio links or made it possible to access to these systems with multiple communication channels and to use a bigger bandwidth in the remote control task. This also improved thesystem response time.

In conclusion, IEC 104 standard applies the remote control concepts defined by IEC 60870-5-101 removing the serial header and adding the appropriate headers for the use of TCP/IP channels.

IEC 60870-5-104 USES THE TCP/IP TECHNOLOGY TO ACCOMPLISH THE REMOTE CONTROL TASKS DEFINED BY IEC 60870-5-101

60870 5-101

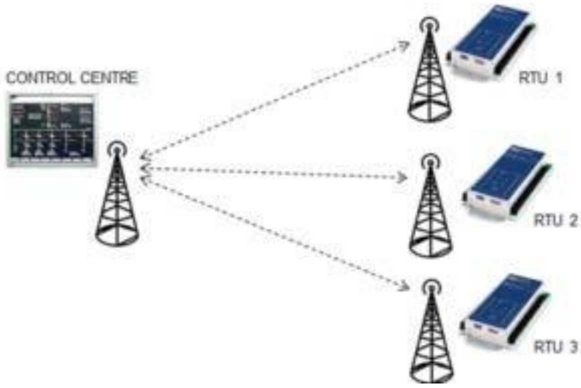
To be able to understand IEC 60870-5-104 we need to learn the basic concepts defined in IEC 60870-5-101.

Communication modes: balanced and unbalanced

Depending on the type of communication channel available: shared (point to multipoint) or dedicated (point to point) we have two different communication modes:

- **Balanced mode.** It is used when a dedicated point to point communication channel is available (telephone connection or dedicated link). The communication is full duplex, and the remote terminal unit can send data without waiting for the control centre to request it. This makes the spontaneousdata transfer faster and so on the control centre update.

- **Unbalance mode.** It is used in point to multipoint links as the radio shared connection. The communication mode is half duplex. The only remote terminalunit that send data is the one that has been requested by the control centre using its specific link address in the data request. The master needs to request cyclically to all the remote terminal units in the channel to know if there is new data waiting to be transferred.

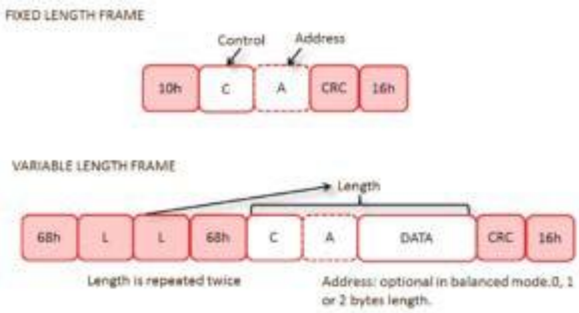


Unbalanced mode used in radio link

The unbalanced mode can also by used in point-to-point channels but it will lost response time due to the lack of spontaneous transmission from the remote terminal units.

Frame formats

IEC 60870-5-101 defines two different types of frames, the fixed length frame (used for control messages) and the variable length frame (used to transport application level messages).



IEC 60870-5-101 frames format

The field marked as data transports the Application Service Data Units (ASDU) that is the container of the remote control services.

Basic application functions

IEC 60870-5-101 defines different types of ASDU to be used in the existing basic application functions:

- Initialization.
- Polling data.

- Periodic transfer.
- Spontaneous event transfer.
- General interrogation.
- Time synchronization.
- Control command.
- Counters.
- Parameters loading.
- Test command.
- File transfer.
- Transfer delay measurements.

1. After the reboot of the remote station, this will notify this event to the control centre by sending an END_ON_INIT ASDU. This message indicates to the control centre that is needed to update its process image of the remote station using the general interrogation process.
2. The general interrogation process allows obtaining the current status of all the digital and analogue signals monitored and included in the general interrogation response by the remote station. This snapshot of the remote station makes it possible to update its process image of the remote station.

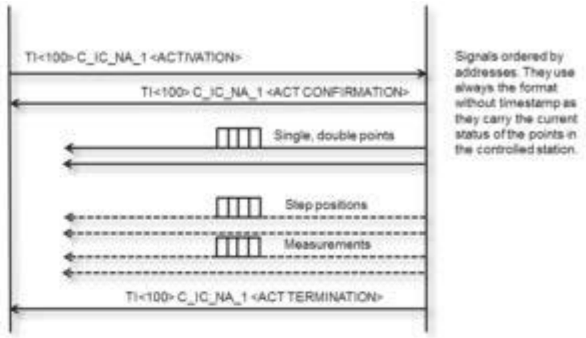


Fig: General interrogation process

3. After the general interrogation process, any change in the status of the variables in the remote station will be sent to the control centre by the use of different mechanisms as the periodical transfer mechanism (used with analogue measurements only) or the spontaneous transfer (used with digital data and measurements with configured dead bands).

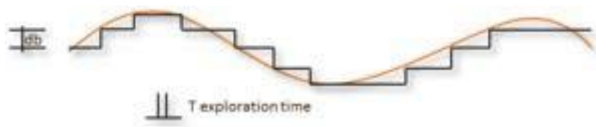
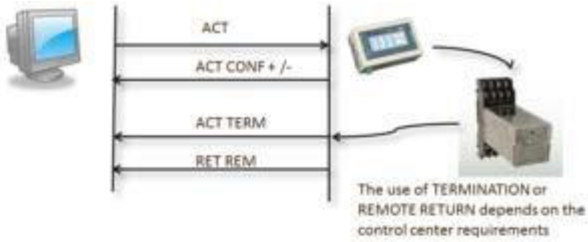


Fig: Spontaneous transfer of measurement with dead band

4. When the remote station includes integrated total as the energy counters, the remote station may send this information on demand or spontaneously depending on the counter mode configured in the system.
5. When an operator requires to modify the system behavior, a command ASDU can be send (C_XX) or a parameter change (P_XX) to act over the controlled system.



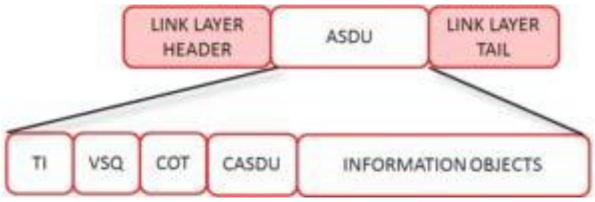
Activation command, confirmation and termination

ASDU – Application Service Data Unit

The messages that are sent by IEC 60870-5-101 use one of the two directions of the communication:

- **Control direction**: from the control centre to the remote station.
- **Monitor direction:** from the remote station to the control centre.

  All the ASDU structures include a common header to identify them:



The ASDU format

- **TI**: Type Identification. Number that identifies the ASDU and then its format and its content.
- **VSQ**: Variable Structure Qualifier. It describes how the information objects are organized.
- **COT**: Cause of Transmission. It includes the reason for sending the ASDU and one byte with an identifier of the control centre.
- **CASDU**: Common Address of ASDU. Application address used to identify the data in the system. Generally a remote terminal unit uses only one CASDU.
- **Information objects**: They include the content of the requested service or the notified information.

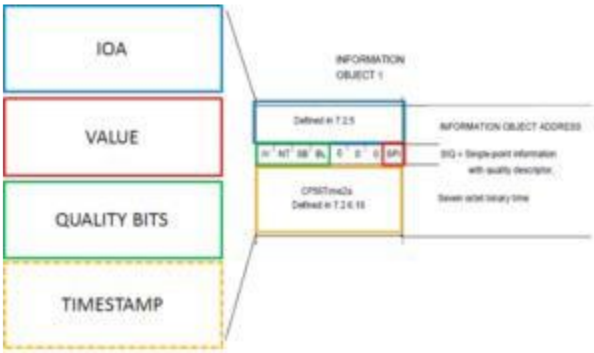
- The standard defines different types of ASDUs to send different kind of information:

- **Process information in monitor direction** that include status values, measurements, step positions, etc. (M_XX_XX_X).
- **Process information in control direction** that includes single commands, double command, step positions and set points (C_XX_XX_X).
- **System information in monitor direction**, M_EI_NA_1 (end_of_init)
- **System information in control direction** that includes the general interrogation commands, counter interrogation, reset, test, read command and time synchronization (C_XX_XX_X).
- **Control direction parameters** that allow to modify the dead bands (P_XX_XX_X)
- **File transfer** (F_XX_XX_X)

Information objects

The format of an information object included the address of the object (IOA), the field

value, the quality of the information, and optionally the timestamp.



The format of the information object

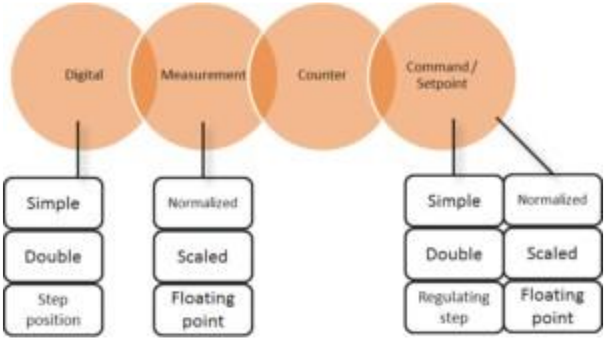
Information identification

Each data point in an IEC 60870-5-101/104 system is identified by two addresses: the common address of application (CASDU) and the information object address (IOA).

Information object types

The information of the remote terminal unit can be divided into categories:

- Digital signals.
- Analogue signals.
- Counters.
- Commands and settings.



Basic information object types

Quality bits in the signals

All the data objects include a quality bit IV that indicates if the value is valid or invalid. At the same time, depending on the data type, several other quality bit are available.

- Substituted (SB) indicates if the value source is the field or if the value was substituted.
- Blocked (BL): indicates that the data point is blocked.
- Overflow (OV): indicates that a measurement is out of range.

Information time stamping

During the general interrogation, the information is sent without time stamping as it only includes the current value of the information of the remote terminal unit. When the remote terminal units send spontaneous ASDUs it uses ASDUs with timestamps so the control centre can create a sequence of events with the chronology that happened in all the remote terminal units.

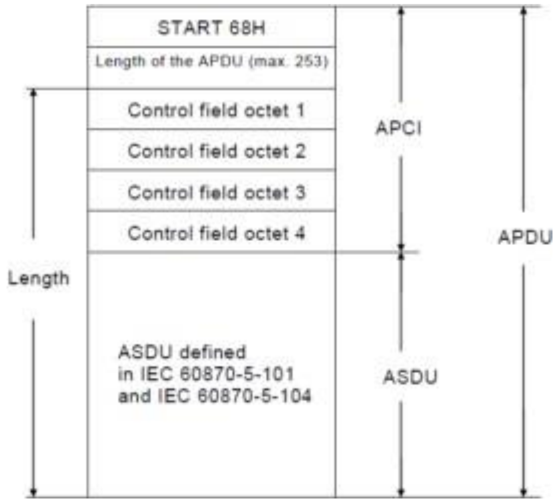
IEC 60870 5-104 standard

IEC 60870-5-104 uses TCP/IP channels with full-duplex communication (near to the balanced mode in IEC 60870-5-101).

While IEC 60870-5-101 wait for a confirmation of each message sent, IEC 60870-5-104 assumes that the channel is stable and a maximum number of K messages can be sent without waiting for confirmation from the opposite station.

IEC 60870 5-104 frame format

IEC 60870-5-104 removes the serial header and adds its own header called APCI (Application Protocol Control Information).



APCI header in IEC 60870-5-104

The first two bits in the first byte of the APCI header are used to identify 3 types of frames:

- **U Frame**. These control frames manage the traffic exchange over the TCP channel. They include a START message to allow the traffic flow, a STOP message to block further communication and a TEST message to check if the connection is alive.
- **I Frame.** These frames transport application data (ASDUs).
- **S Frame**. The Supervisory frames indicate to the opposite station the number of the last frame received properly. They are used as an acknowledge of a setof messages in order to indicate that the transmission of data can continue.

Redundancy groups in IEC 60870-5-104

IEC 60870-5-104 allows the definition of redundancy channels over TCP/IP. The control centre establishes several connections at the same time (using different physical channels) and it activates one of these connections while the others are in the STOPPED state waiting for being STARTED when the communication in the active channel is lost.

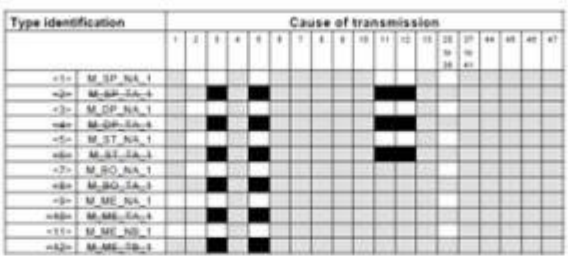
Differences with the application layer in IEC 60870-5-101

IEC 60870-104 does not accept the use of any ASDU using relative timestamp with the information element CP24Time2A (24 bits). The absolute time stamp with the information element CP56Time2A (56bits) must be used.

Trying to synchronize a remote station through a TCP/IP channel with the time synchronization ASDU is not deterministic. With the TCP/IP profile used by IEC60870-5-104 time synchronization prefers to use other protocols as SNTP or NTP (Network Time Protocol). When high accuracy is needed usually a GPS clock with IRIG-B or PTP is the choice selected.

Interoperability

The interoperability document indicates which basic application functions are available, and their supported options, at the same time this document identifies the supported ASDU and cause of transmission (COT) for each one.



Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1																			
<2>	~~M_SP_TA_1~~																			
<3>	M_DP_NA_1																			
<4>	~~M_DP_TA_1~~																			
<5>	M_ST_NA_1																			
<6>	~~M_ST_TA_1~~																			
<7>	M_BO_NA_1																			
<8>	~~M_BO_TA_1~~																			
<9>	M_ME_NA_1																			
<10>	~~M_ME_TA_1~~																			
<11>	M_ME_NB_1																			
<12>	~~M_ME_TB_1~~																			

Interoperability document section

Using the interoperability document (provided by the vendor of the remote terminal unit) the control centre knows how to configure the communication with that device.

At the same time, using this document the control centre may know if the remote terminal unit is compatible with its required functions.

During the system integration process, the compatible options must be selected comparing the control centre and the remote station interoperability documents.

Profiles

The profiles are specifications that select a specific set of options from the available ones in the standard EC 60870-5-101/104. Usually the utility profiles also define addressing ranges for the different types of data and even specific points configured with special uses in their systems.

The motivation for the profiles is the limitation of the available options to select the best one according to the utility needs and also to solve any issue where the standard was not accurate. As an example a profile can be the selection of sending the analogue measurements periodically using the scaled value format, whilst a different profile may request to send them using spontaneous transmission and the floating point ASDU. The remote terminal unit manufacturer must check that the device fulfil the requirements of the profile specified by the utility before their devices can be installed in their system.

Usually the utility will request that the remote terminal unit is tested to be sure that their profile is implemented. This conformance test is performed with a test specification provided by the utility.

Testing specifications with IEC 60870 5-104

IEC defines **IEC 60870-5-601/604** document with the basis test procedures to validate controlling and controlled station that use the standards IEC 60870-5-101/104.
The test cases to be executed depend on the device capabilities defined in their interoperability document.

Security inclusion with IEC 60870 5-104

IEC 60870-5-101/104 protocols do not include authentication of the data sent, so they are vulnerable to unauthorized connection or data modification throwing man-in-the-middle attacks. Usually the security measures consist of tables with list of authorized IP addresses, private networks and firewalls in the remote station.

These measures nowadays are considered to be quite poor and the experts in the TC 57 WG15 are working to develop extension to provide security to the remote-control communications.

The main topics related to the security of IEC 60870-5-101/104 protocols are described in the technical specification IEC 62351-5. The technical specification IEC 60870-5-7 describes the new ASDU messages used. At the same time the document IEC 62351-100-1 describes the test procedures to validate the secure implementations.

COMMON TERMS

- ***ASDU*** *– Application Service Data Unit. Data structure that holds application layer information to exchange between a control centre and a remote terminal unit.*
- ***DNP3*** *– Distributed Network Protocol version 3. Protocol used for automation and remote control communication with serial and TCP-IP capabilities that is used in substation automation and the communication with control centers.*
- ***IEC*** *– International Electrotechnical Commission – International organization that develops standards related to the energy sector.*
- ***IEC 60870-5-101/104 –*** *Protocol serial or TCP/IP to exchange data from a substation to the control centre.*
- ***IED*** *– Intelligent Electronic Device – Any equipment with communication capabilities used to automate a system.*
- ***RTU*** *– Remote Terminal Unit – Device that gather the information of a whole system and send it to the control centre using protocols as DNP3 or IEC 60870-5-101/104.*

Vol. II Part – A

Appendix – C

ICCP Profile

ICCP interoperability profile of a typical Control Centre

Sample ICCP Association Information Exchange Form

The attached ICCP Association Information Exchange Form has been created to facilitate ICCP associations between ICCP nodes. ICCP node administrators should fill out this form using their own setup information. Thus, the form will contain information supplied by *company-A* to *company-B* detailing the parameters needed during *company-B's* ICCP association configuration. Note that similar information needs to be supplied by *company-B* to *company-A*.

The fields are marked as Mandatory, Recommended, or Optional. Mandatory fields are required in order to create an association. Recommended fields should generally be filled in if applicable. For example, an OSI NSAP is only required if using an OSI stack. Optional fields can be filled in for instance to help with troubleshooting if connection or data transmission errors occur. Following tables are informative tables may be modified in future, if required.

Revision history:

Version Date	Comments

ICCP Association Information Exchange Form

Date:

Company A:

Company B:

General Notes:
Sample ICCP format has been attached, actual input will be provided during execution of project

Table 1: Company-wide / Server independent information

1. ICCP vendor and platform the name of the Company-A's ICCP vendor, vendor software version, as well what operating system and hardware platform used for the ICCP servers.	M	e.g Name: XXXX Version: Version 3.0 Platform: XX
2. Number of possible ICCP servers: This is the total number ofICCP servers that may be available to a remote client to associate with. Include backup servers if they have unique addresses. This number should equal the number of copies of Table 2 included in this form. Typically, 1-10	R	e.g. 2
3. Company A's domain name: The domain name which company-B will use to access data on Company-A's ICCP node. Recommended to be the 4-character ISN node name ofCompany-B.	M	e.g., xxx – St yyy Between RSCC and SLDC
4. Requested Company B's Domain name: The Domain nameon company B's ICCP node which Company A requests to becreated. This is only a request as this name is designated by Company-B. recommended to be the 4-character node name of Company-A. this is the only entry on these forms that refersto Company B's ICCP node.	O	
5. Bilateral table ID: Company A's bilateral table name used when Company B is accessing Company A's data (e.g., "1.1").	M	e.g., Bilat_ID_St SLDC
6. Supported ICCP services: A list of the conformance blockssupported by the server (e.g., Blocks 1, 2).	M	BLOCK 1,2,4,5
7. ICCP version: The version of ICCP running on the server(e.g., TASE.2 Version 1996-08).	M	TASE.2 Version 1996-08
8. Shortest periodic interval: Time in seconds at which Company A's data is being updated. Typically, 10 seconds.	O	10 seconds also configurable, but greater than 1 second.

9. ISN style NSAP's: A collection of NSAP's have been assigned by ICI for use by ISN ICCP nodes. These all use a particular addressing scheme called ISN style NSAP's. Alternatively, some ICCP nodes are using TCP/IP only or areusing their own NSAP addressing scheme. Typically, "yes".	R	TCP/IP is used
10. OSI routing Company A's router: If you are using ISN style NSAP's, this 4-byte number is part of the company-B's router configuration and consists of a 2-byte Domain ID and a 2-byte Area ID. If you are using OSI, but not using ISN style NSAP's then enter the full hex string. If you areusing TCP/IP, then leave this blank.	R	
11. IP address of the WAN port on Company A's router. If youare using TCP/IP, this field is either a fully qualified domain name or a 12-integer number delimited with periods.	R	e.g .xxxxxx 7-64kbps WAN Links for one chart State
12. Transport Layer Ack Time: This field indicates a maximum time in seconds that can elapse between receipt of a TPDU byTransport from the network layer and the transmission of the corresponding acknowledgment. Typically, 5 seconds.	O	Default
13. Transport Layer Retransmission Time: This field indicatesthe maximum time in seconds Transport will wait for an acknowledgment before retransmitting a TPDU. Typically, 10 seconds.	O	Default
14. Transport Layer Window Time: This field indicates a maximum time in seconds that Transport will wait before retransmitting up-to- date window information. Typically, 10seconds.	O	Default
15. Number of Retries: This field indicates the maximum number of attempts to retransmit a TPDU before issuing aDisconnect Request. Typically, 6.	O	Default
16. Maximum MMS PDU size. Size in bytes of the maximum MMS protocol data unit. Typically, 8k bytes or more.	O	32 Kbytes

Table 2: ICCP Server specific information

(This table should be duplicated for each ICCP server installed)

1. Server name: The name by which company-A refers to this server. This field is not electronically transmitted during any ICCP transactions, but is only here to facilitate verbal communication between Company A and Company B.	O	e.g. Std Server @ ReBG, LOCC
2. Server number: “1” if this is the primary server, “2” if this is the first backup, etc.	R	e.g. xxxxx04 – 1 yyyyy06 - 2
3. IP network address: If you are using TCP/IP, this optional field is the IP address for this ICCP server if TCP/IP can be used as the network transport.	R	e.g., xxx.xx.xx.x
4. AP Title: Optional Object identifier representing the Application Process Title given to this application	R	To be provided
5. AP Invoke ID A long integer used to identify an invocation instance of the application process. Typically, not specified.	O	e.g., Client – 100 Server - 100
6. AE Qualifier A long integer (32 bit signed) is usedto qualify the application entity.	O	e.g., Client – 1 Server - 101
7. AE Invoke ID Used to identify an invocation instance of the application entity. Typically, not specified.	O	e.g., Client – 1 Server - 101
8. Presentation Selector (PSEL) 2- or 4-byte number used to select the correct instance of the presentation layer (e.g., 00 09 or 00 00 00 09).	R	To be provided
9. Session Selector (SSEL) 2- or 4-byte number usedto select the correct instance of the session layer (e.g., 00 09 or 00 00 00 09).	R	e.g., 00 01
10. Transport Selector (TSEL) 2- or 4-byte number used to select the correct instance of the session layer (e.g., 00 09 or 00 00 00 09).	R	e.g., 00 01

11. Complete NSAP A number that represents the OSI network address for Company A's ICCP node. The NSAP can be upto 20 bytes long. For ISN nodes, the first 7 bytes should be (in hex)	R	To be provided
12. Association type "Single direction Client-Server": Enter this if Company A's and Company B's ICCP nodes act aseither Client or Server over one association. Information can be sent in only one direction per association. The client must initiate the association. "Dual direction Client-Server": Enter this if Company A's and Company B's ICCP nodes act as Client and Server over one association. Information can be sentin either direction per association. The association type is determined by prior agreement between the two users. Typically, "Dual direction Client-Server".	R	e.g., Single Direction Client Server
13. Association Initiation: This field is only used if the association type is "Dual direction Client-Server" and indicates which ICCP node shall initiate the association (e.g., company-A). The initiator of the association is determined by prior agreement between the two users.	R	Not applicable

Appendix A: Sample Explanation of ISN Style NSAP's

ISN Style NSAP have the following form (in hex):

39 840f 80 113826 0000 rrrr aaaa dddddddddddd nn

The first byte contains the Authority Format ID (AFI) where 39 is for ISO

The next two bytes contain Initial Domain ID (IDI) where 840F is for USA.

The next byte contains the Domain Format ID (DFI) where 80 is for GOSIP style format.

The next three bytes contain the organization ID where 113826 is for NERC.

The next two bytes is a reserved field and should be set to 0000

rrrr = Routing Domain ID (Contact NERC for this value)

aaaa = Area (Contact NERC for this value)

dddddddddddd = Station ID (see below)

nn = NSEL (see below)

ISN Style Station ID Addressing Standard

The next to last 6 bytes of the NSAP contain the Station ID. The Station ID format is:

Bytes 1-4 ASCII code in hex of the registered Site ID of the ISN (or other ICCP) Node with padded underscore(s) as needed.

Byte 5 ASCII code in hex of the node number on which the server is running. For example, if the node number is equal to '1' then byte 5 should contain hex 31.

Byte 6 ASCII code in hex indicating the application specification of the Protocol: Hex 49 for ICCP

Examples:

SC 1I 53	43	5F	5F	31	49	
ECAR1I	45	43	41	52	31	49
ECAR2I	45	43	41	52	32	49

ASCII to Hex and Conversion Table for Station ID's:

ASCII	Hex	ASCII	Hex	ASCII	Hex	ASCII	Hex
_	5F	9	39	I	49	R	52
1	31	A	41	J	4A	S	53
2	32	B	42	K	4B	T	54
3	33	C	43	L	4C	U	55
4	34	D	44	M	4D	V	56
5	35	E	45	N	4E	W	57
6	36	F	46	O	4F	X	58
7	37	G	47	P	50	Y	59
8	38	H	48	Q	51	Z	5A

Note: NSAP's are always specified in hex while the AP Title standard in Appendix B consists of a set of decimal numbers. Use this table to translate your site id into hex for the station ID portion of your NSAP's.

The Network Selector or NSEL is the last byte of the NSAP and is used to select the correct instance of the Network layer. Some DEC net/OSI systems will automatically assign this a value (20 hex for Phase IV NSP transport, 21 hex for OSI transport TP4). Other OSI stacks do not impose this requirement. The recommended value for systems on which it is not automatically assigned is 01.

Appendix B: Mandatory AP Title Standard

The AP Title is used by some ISO applications to determine what application is calling since NSAP's, TSEL's, SSEL's and PSEL's of the caller may not passed to applications upon association. The AP Title consists of 9 16-bit decimal numbers:

Field Name	1	2	3
Field format	One single 16 bit decimal integer)	One 16 bit decimal integer	Seven 16-bit decimal integers
Required value in decimal	2 (joint-iso-ccitt)	16 (country based naming hierarchy)	3826 XXXX XXXX XXXX XXXX YYYY 0073 (3826 is the abbreviated NERC org ID used to specify ISN applications), XXXX XXXX XXXX XXXX is for the registered ISN node ID in decimal (one 16 bit decimalnumber for each ASCII character in the site ID including padding underscores), YYYY is the for the node number (one 16 bit decimal number), the last 16 bit numberis an application specification where decimal 0073 indicates ICCP.)

For example, an ICCP application at MAIN1 would have an AP Title of:
0002 0016 3826 0077 0065 0073 0078 0049 0073
Note: Some ICCP vendors do not provide a user interface for setting AP Titles. In this case the user may be required to manually edit a Directory Information Base ASCII file.

ASCII to Decimal Conversion Table:

ASCII	DEC	ASCII	DEC	ASCII	DEC	ASCII	DEC
_	95	9	57	I	73	R	82
1	49	A	65	J	74	S	83
2	50	B	66	K	75	T	84
3	51	C	67	L	76	U	85

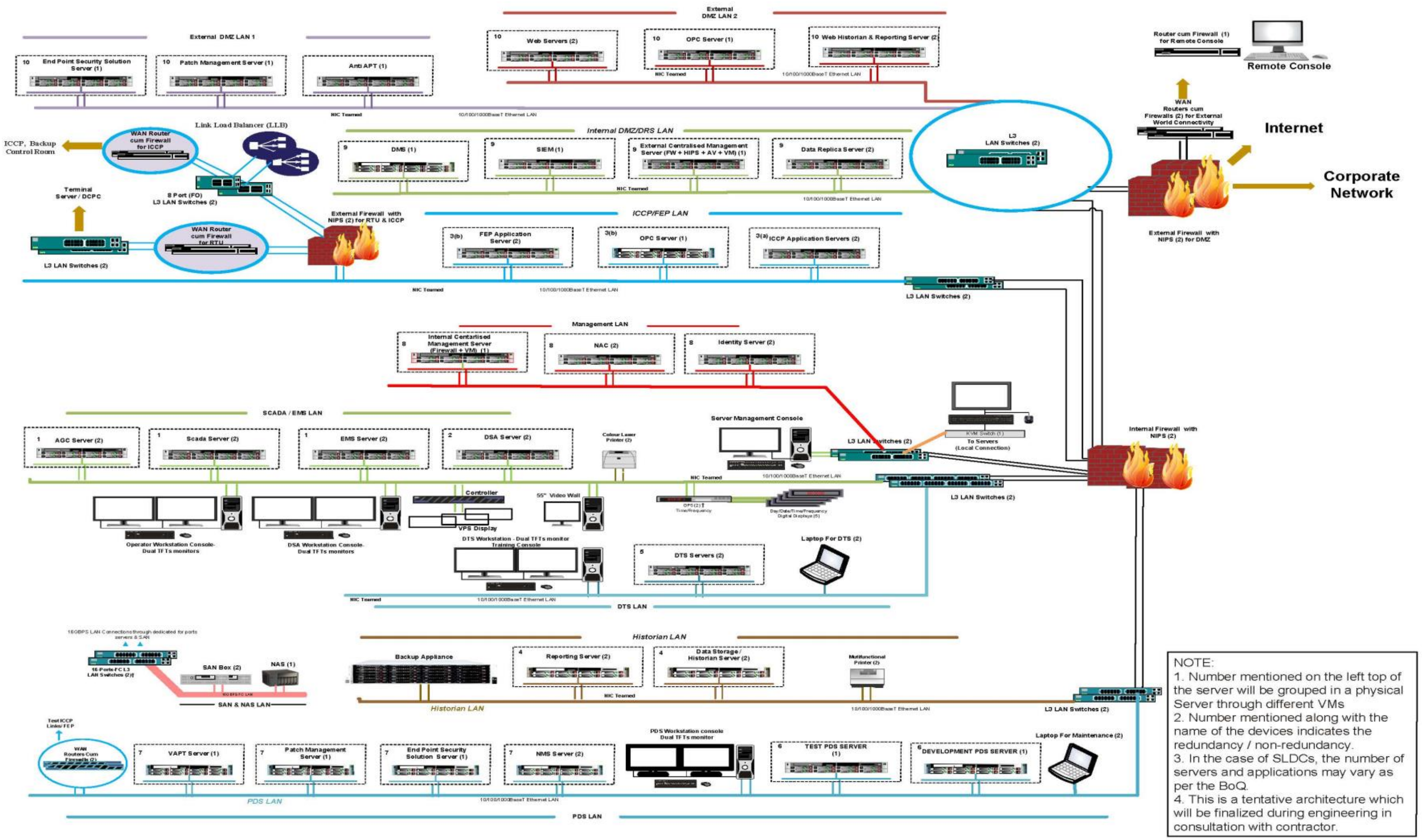
4	52	D	68	M	77	V	86
5	53	E	69	N	78	W	87
6	54	F	70	O	79	X	88
7	55	G	71	P	80	Y	89
8	56	H	72	Q	81	Z	90

VOL. II, PART - A

APPENDIX - D

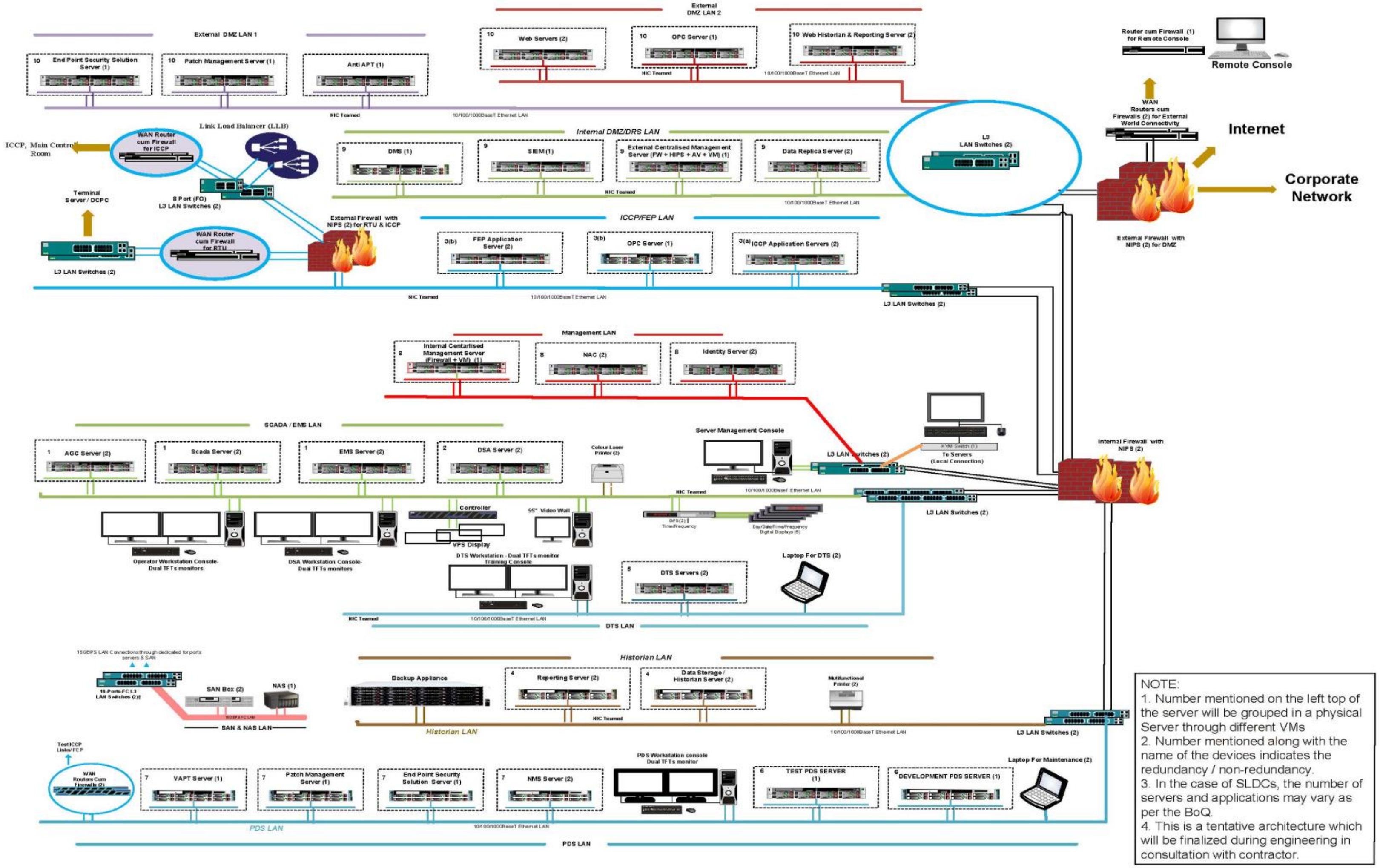
NETWORK ARCHITECTURE

Network Architecture for RLDC/SLDC MAIN CONTROL CENTRE



NOTE:
1. Number mentioned on the left top of the server will be grouped in a physical Server through different VMs
2. Number mentioned along with the name of the devices indicates the redundancy / non-redundancy.
3. In the case of SLDCs, the number of servers and applications may vary as per the BoQ.
4. This is a tentative architecture which will be finalized during engineering in consultation with contractor.

Network Architecture for RLDC/SLDC BACK UP CONTROL CENTRE



NOTE:
1. Number mentioned on the left top of the server will be grouped in a physical Server through different VMs
2. Number mentioned along with the name of the devices indicates the redundancy / non-redundancy.
3. In the case of SLDCs, the number of servers and applications may vary as per the BoQ.
4. This is a tentative architecture which will be finalized during engineering in consultation with contractor.

Vol. II, Part-A

Appendix - E

Implementation Schedule

Appendix-E: Project Implementation Schedule- 18 Months (Months after letter of Award-LOA)

S No	Task Name	Task Completion by	Months after Letter of Award (LOA)																	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	(SCADA/EMS & Aux Power Package)	**18 Months**																		
1	***Letter of Award (LOA)***	***0 days***																		
2	***Testing of RTU and ICCP***	***3rd Month***																		
3	***Engineering***	***6th Month***																		
4	***Data Base Development***	***8th Month***																		
5	***Factory Testing of Equipment's***																			
(a)	SCADA/EMS Control Centre	***10th Month***																		
(b)	*Auxiliary Power Supply System*	***7th Month***																		
6	***Supply, Installation and Commissioning of Equipment's***																			
(a)	*Auxiliary Power Supply System*	***9th Month***																		
(b)	SCADA/EMS Control Centre	***12th Month***																		
7	***Site Acceptance Testing of Equipment's***																			
(a)	*Auxiliary Power Supply System*	**12th Month**																		
(b)	SCADA/EMS Control Centre	***15th Month***																		
8	***Parallel Operation of Existing System and New System & Availability Test***	***18th Month***																		
9	***Taking Over***	***18th Month***																		

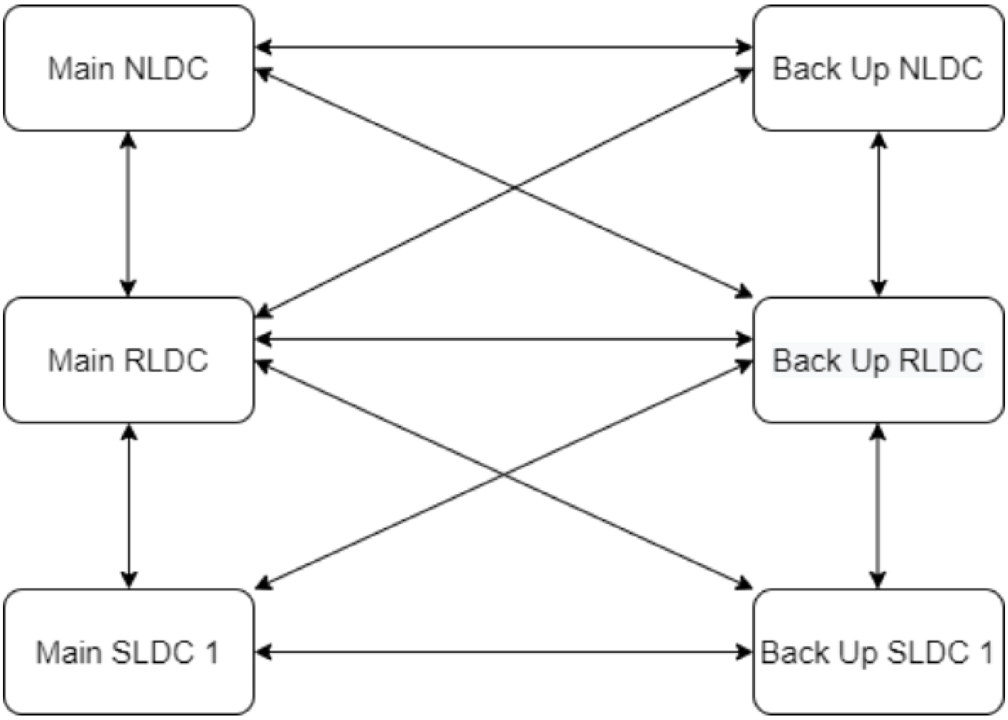
Vol. II, Part-A

Appendix-F

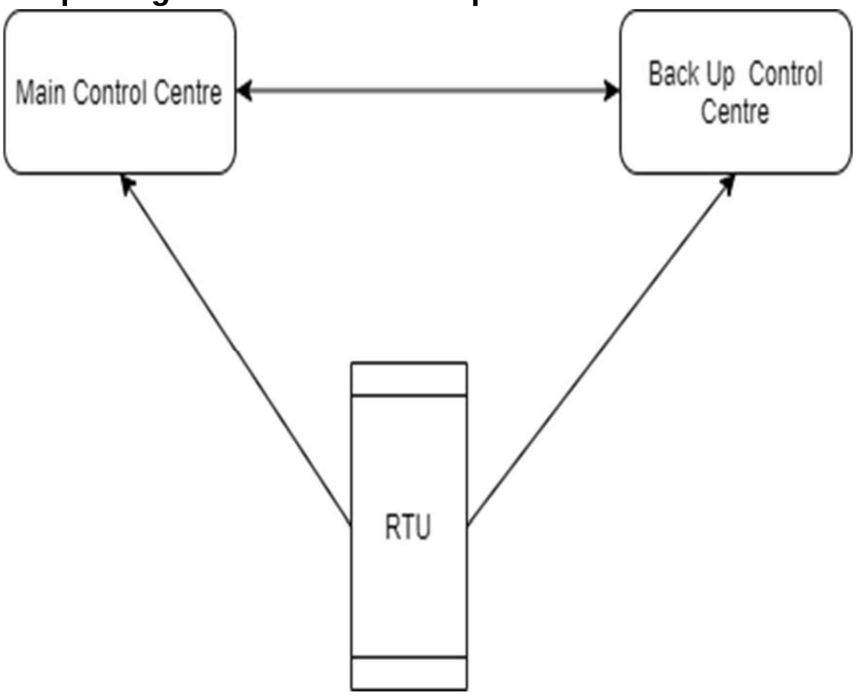
ICCP, RTU and Historian Configuration

ICCP, RTU and Historian Configuration

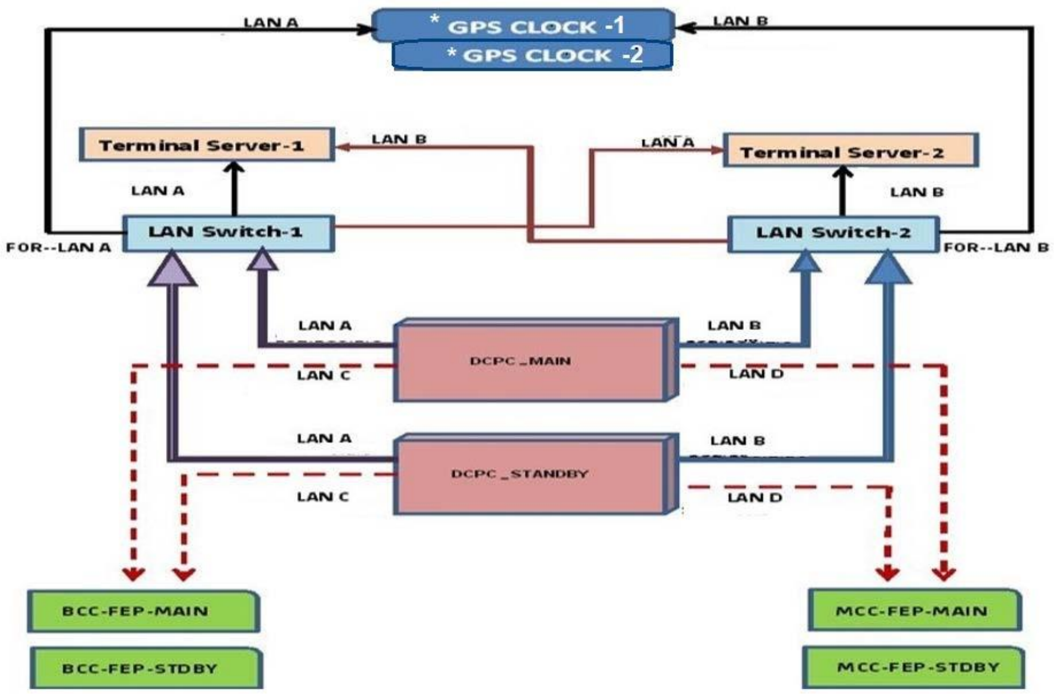
A. ICCP data reporting to Main and Back up control centre



B. RTU reporting to Main and Back up Control centre

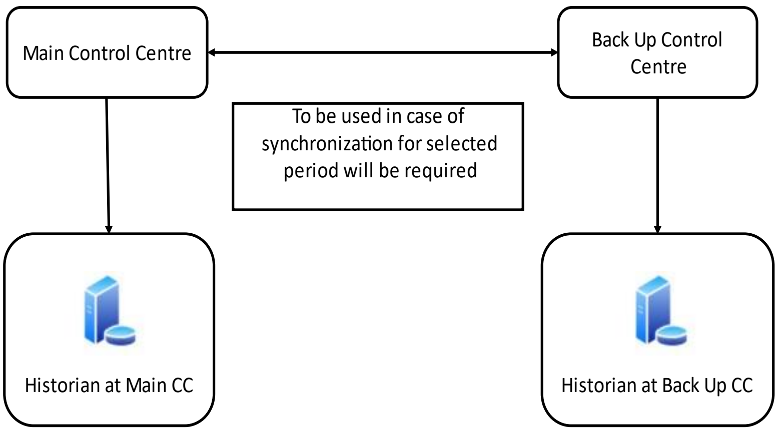


C. DCPC Hardware Connectivity Diagram



* Both the GPS clocks will work in active active mode and systems will synchronize with NTP accordingly

D. Historian data reporting to Main and Back up control center



Vol. II, Part-A

Appendix-G

Cyber Security Audit

Cyber Security Audit

A. Vulnerability Assessment

To identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system by using various automated tools along with manual verification of identified issues. VA shall be comprehensive but not limited to following activities:

- ***Network Scanning***: Contractor shall identify active hosts on a network, for the purpose of simulating attack and also for network security assessment with the help of suitable procedure/tools including but not limited to:

  a. Examine Name server responses
  b. Review the outer wall of the network
  c. Review tracks from the target organization
  d. Review Information Leaks

- ***Port Scanning***: To find the active ports on server/equipment's, port addresses on a host, Contractor shall perform the following but not limited to:

  a. Error Checking
  b. Enumerate Systems
  c. Enumerating Ports
  d. Verification of Various Protocol Response
  e. Verification of Packet Level Response

- ***Port Sweep***: To scan multiple hosts for a specific listening port for potential vulnerabilities.
- ***System & OS Fingerprinting***: To guess the system information i.e., type and version of OS, patch version etc.
- ***System Identification & Trusted System (SITS) Scanning***: Contractor shall perform the SITS scanning which would include but not limited to the following:

  a. Match each open port to a service and protocol.
  b. Identify server uptime to latest patch releases.
  c. Identify the application behind the service and the patch level using fingerprints.
  d. Verify the application to the system and the version.
  e. Locate and identify service remapping or system redirects.
  f. Identify the components of the listening service.
  g. Use UDP-based service and Trojan requests to all the systems in the network.

- ***Malware Scanning***: Contractor shall do exhaustive scanning for hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

- ***Spoofing***: Contractor shall assess the scope of potential spoofing attacks i.e. IP, ARP etc and other applicable ones in the office environment
- ***Security Policy Review***: Contractor shall carry out the review & assessment of Security Policies already in place in UTMs/Firewalls, routers & switches installed in the organization.
- ***Services Probing***: Anti-Virus and Trojan
- ***Service Fingerprinting***: The Contractor shall do the following:
  a. Examine system responses to determine operating system type and patch level.
  b. Examine application responses to determine operating system type and patch level.
  c. Verify the TCP sequence number prediction for each live host on the network.
  d. Search job postings for server and application information from the target.
  e. Search tech bulletin boards and newsgroups for server and application information from the target.
  f. Match information gathered to system responses for more accurate results.

- ***Access Control Mapping***: ACL has to be reviewed and recommended for improvement.
- ***Assessment of OS Hardening***: Contractor shall carry out the assessment of OS hardening to check & explore the gap in hardening, patch management etc.
- ***Denial Of Service (DOS) Attacks***: Following points shall be looked for DoS attack:
  a. Verify that administrative accounts and system files and resources are secured properly and all access is granted with "Least Privilege".
  b. Check the exposure restrictions of systems to non-trusted networks
  c. Verify that baselines are established for normal system activity
  d. Verify what procedures are in place to respond to irregular activity.
  e. Verify the response to SIMULATED negative information (propaganda) attacks.
  f. Test heavy server and network loads.

- ***DDOS Attacks***: All the steps as mentioned for DoS attack shall be verified.
- ***Authorization Testing***: Contractor shall do the authorization & authentication testing for the present AD system.
- ***Lockout Testing***: To mitigate the brute force attack etc., lockout testing must be carried out.
- ***Password Cracking***: To mitigate the brute force attack, cryptographic attack etc., Password cracking testing must be carried out.
- ***Cookie Security***: Contractor shall review the cookie settings and recommend the best practice for making the environment secure.
- ***Containment Measure Testing***: The Contractor shall perform this test also wherever applicable.
- ***DMZ Network Architecture Review***: Contractor shall review the present DMZ Network Architecture and recommend for the improvement, if any.
- ***Server Assessment (OS Security Configuration)***: Contractor shall review the present configuration of servers and recommend for the improvement, if any.

- ***Man in the Middle attack***: To rule out the possibilities of eavesdropping the MIMA shall be accrued out.
- ***Directory Traversal***: Directory Traversal is a type of HTTP exploit that is used by attackers to gain unauthorized access to restricted directories and files.
- ***Linux Hacking***: Assessment of the security risk associated with systems running on Linux platform, if any.
- ***Keyloggers***: Keyloggers are a form of spyware where computer users are unaware their actions are being tracked.
- ***Rootkit***: Assessment of the systems to see the presence or probability of presence of rootkit.
- ***Botnet***: Assessment of the system to see the presence of botnet.
- ***Any other attacks & Scenario Analysis***: Apart from all the above-mentioned line item if any activity required during the testing period due to new identified vulnerability, Contractor has to carried out.

B. Penetration Testing (Internal and External)

- Trusted System Scanning
- Network Scanning for known Trojans
- Administrator Privileges Escalation Testing
- Services Probing
- Attempt ARP poisoning
- Attempt MAC flooding
- Attempt DNS poisoning
- Identification of Services
- Short Listing of Crucial IPs
- Identification of Operating System
- Vulnerability Research and Verification
- Password Cracking
- IDS/IPS testing
- Router, Switch & Firewall testing
- DOS/DDOS Testing
- Various other tests and attacks
- IP spoofing
- Any other attacks

Vol. II, Part-A

Appendix-H

Details of Control Centers–Location

Details of New Control Centres under this Project

S. No.	SLDC	Main	Backup
1	OPTCL	Bhuvneshwar	Meeramandali
2	DVC	Howrah, DVC headquarter	Maithon
3	WBSETCL	Howrah	Abhikshan Bhawan
4	Sikkim	Gangtok	Melli
5	Bihar	Patna	Chandauti
6	Jharkhand	Sarwal	Kusai
7	ERLDC	ERLDC, Kolkata	Guwahati

Details of DCPC/Terminal server

S. No	Control Centres	Number of DCPC/Terminal server	Location of DCPC/Terminal server
1	ERLDC	2	Durgapur
2	JUSNL	2	

Vol. II, Part-A
Appendix – I
Details of Inter Control Centre Communication

DETAILS OF INTER CONTROL CENTRE COMMUNICATIONS (Tentative)

S No.	Control Center	Inter Control Centre Association		Bandwidth and No. of Communication Channels
1.	Main ERLDC	1.	Main ERLDC- Backup ERLDC (Main Back up Link)	
		2.	Main ERLDC- Main NLDC-India	
		3.	Main ERLDC – SLDC 1	
		4.	Main ERLDC – SLDC 2	
		5.	Main ERLDC – SLDC 3	
		6.	Main ERLDC – SLDC 4	
		7.	Main ERLDC – SLDC 5	
		8.	Main ERLDC – SLDC 6	
		9.	Main ERLDC – SLDC..n	
		10.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		11.	………..Any Other Association………..	
2.	Backup ERLDC	1.	Backup ERLDC- Main ERLDC (Main Back up Link)	
		2.	Backup ERLDC- Backup NLDC-India	
		3.		
		4.	Backup ERLDC - SLDC1	
		5.	Backup ERLDC - SLDC 2	
		6.	Backup ERLDC - SLDC 3	
		7.	Backup ERLDC - SLDC 4	
		8.	Backup ERLDC - SLDC 5	
		9.	Backup ERLDC - SLDC 6	
		10.	Backup ERLDC - SLDC ..n	
		11.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		12.	………..Any Other Association………..	
3.	DVC Main SLDC	1.	DVC Main SLDC- DVC Backup SLDC (Main Backup Link)	
		2.	DVC Main SLDC- Main ERLDC	
		3.	DVC Main SLDC- Backup ERLDC	
		4.	DVC Main SLDC- DISCOM 1	
		5.	DVC Main SLDC- DISCOM 2	

		6.	DVC Main SLDC- DISCOM 3	
		7.	DVC Main SLDC- DISCOM 4	
		8.	DVC Main SLDC- DISCOM ..n	
		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	………..Any Other Association………..	
4.	DVC Backup SLDC	1.	DVC Backup SLDC- DVC Main SLDC (Main Backup Link)	
		2.	DVC Backup SLDC-Main ERLDC	
		3.	DVC Backup SLDC- Backup ERLDC	
		4.	DVC Backup SLDC - DISCOM1	
		5.	DVC Backup SLDC - DISCOM 2	
		6.	DVC Backup SLDC - DISCOM 3	
		7.	DVC Backup SLDC - DISCOM 4	
		8.	DVC Backup SLDC - DISCOM.. n	
		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	………..Any Other Association………..	
5.	WBSETCL Main SLDC	1.	WBSECTL Main SLDC – WBSECTL Backup SLDC (Main Backup Link)	
		2.	WBSETCL Main SLDC- Main ERLDC	
		3.	WBSETCL Main SLDC- Backup ERLDC	
		4.	WBSETCL SLDC- CESC Kolkata	
		5.	WBSETCL SLDC- DISCOM 1	
		6.	WBSETCL SLDC- DISCOM 2	
		7.	WBSETCL SLDC- DISCOM 3	
		8.	WBSETCL SLDC- DISCOM ..n	
		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	………..Any Other Association………..	
6.	WBSETCLBackup SLDC	1.	WBSECTL Backup SLDC – WBSECTL Main SLDC (Main Backup Link)	

		2.	WBSETCL Backup SLDC- Main ERLDC	
		3.	WBSETCL Backup SLDC- Backup ERLDC	
		4.	WBSETCL Backup SLDC- CESC Kolkata	
		5.	WBSETCL Backup SLDC- DISCOM 1	
		6.	WBSETCL Backup SLDC- DISCOM 2	
		7.	WBSETCL Backup SLDC- DISCOM 3	
		8.	WBSETCL Backup SLDC- DISCOM ..n	
		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	………..Any Other Association………..	
7.	SIKKIM Main SLDC	1.	SIKKIM Main SLDC- SIKKIM Backup SLDC (Main Backup Link)	
		2.	SIKKIM Main SLDC- Main ERLDC	
		3.	SIKKIM Main SLDC- Backup ERLDC	
		4.	SIKKIM Main SLDC- DISCOM 1	
		5.	SIKKIM Main SLDC- DISCOM 2	
		6.	SIKKIM Main SLDC- DISCOM 3	
		7.	SIKKIM Main SLDC- DISCOM 4	
		8.	SIKKIM Main SLDC- DISCOM ..5	
		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	………..Any Other Association………..	
8.	SIKKIM Back up SLDC	1.	SIKKIM Backup SLDC- SIKKIM Main SLDC (Main Backup Link)	
		2.	SIKKIM Backup SLDC- Main ERLDC	
		3.	SIKKIM Backup SLDC- Backup ERLDC	
		4.	SIKKIM Main SLDC- DISCOM 1	
		5.	SIKKIM Main SLDC- DISCOM 2	
		6.	SIKKIM Main SLDC- DISCOM 3	
		7.	SIKKIM Main SLDC- DISCOM 4	

		8.	SIKKIM Main SLDC- DISCOM..5	
		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	………..Any Other Association………..	
9.	OPTCL Main SLDC	1.	OPTCL Main SLDC- OPTCL Backup SLDC (Main Backup Link)	
		2.	OPTCL Main SLDC- Main ERLDC	
		3.	OPTCL Main SLDC- Backup ERLDC	
		4.	OPTCL Main SLDC- DISCOM 1	
		5.	OPTCL Main SLDC- DISCOM 2	
		6.	OPTCL Main SLDC- DISCOM 3	
		7.	OPTCL Main SLDC- DISCOM 4	
		8.	OPTCL Main SLDC- DISCOM 5	
		9.	OPTCL Main SLDC- DISCOM..n	
		10.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		11.	………..Any Other Association………..	
10.	OPTCL Backup SLDC	1.	OPTCL Backup SLDC- OPTCL Main SLDC (Main Backup Link)	
		2.	OPTCL Backup SLDC- Main ERLDC	
		3.	OPTCL Backup SLDC- Backup ERLDC	
		4.	OPTCL Backup SLDC- DISCOM 1	
		5.	OPTCL Backup SLDC- DISCOM 2	
		6.	OPTCL Backup SLDC- DISCOM 3	
		7.	OPTCL Backup SLDC- DISCOM 4	
		8.	OPTCL Backup SLDC- DISCOM 5	
		9.	OPTCL Backup SLDC- DISCOM ..n	
		10.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		11.	………..Any Other Association………..	
11.	BSPTCL Main SLDC	1.	BSPTCL Main SLDC- BSPTCL Backup SLDC (Main Backup Link)	
		2.	BSPTCL Main SLDC- Main ERLDC	

		3.	BSPTCL Main SLDC- Backup ERLDC	
		4.	BSPTCL SLDC- DISCOM 1	
		5.	BSPTCL SLDC- DISCOM 2	
		6.	BSPTCL SLDC- DISCOM 3	
		7.	BSPTCL SLDC- DISCOM 4	
		8.	BSPTCL SLDC- DISCOM ..n	
		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	……….Any Other Association……….	
12.	BSPTCL Backup SLDC	1.	BSPTCL Backup SLDC- BSPTCL Main SLDC (Main Backup Link)	
		2.	BSPTCL Backup SLDC- Main ERLDC	
		3.	BSPTCL Backup SLDC- Backup ERLDC	
		4.	BSPTCL Backup SLDC- DISCOM 1	
		5.	BSPTCL Backup SLDC- DISCOM 2	
		6.	BSPTCL Backup SLDC- DISCOM 3	
		7.	BSPTCL Backup SLDC- DISCOM 4	
		8.	BSPTCL Backup SLDC- DISCOM 1..n	
		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	……….Any Other Association……….	
13.	JUSNL Main SLDC	1.	JUSNL Main SLDC- JUSNL Backup SLDC (Main Backup Link)	
		2.	JUSNL Main SLDC- Main ERLDC	
		3.	JUSNL Main SLDC- Backup ERLDC	
		4.	JUSNL Main SLDC- DISCOM 1	
		5.	JUSNL Main SLDC - DISCOM 2	
		6.	JUSNL Main SLDC - DISCOM 3	
		7.	JUSNL Main SLDC - DISCOM 4	
		8.	JUSNL Main SLDC - DISCOM ..n	

		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	………..Any Other Association………..	
14.	JUSNL Backup SLDC	1.	JUSNL Backup SLDC- JUSNL Main SLDC (Main Backup Link)	
		2.	JUSNL Backup SLDC- Main ERLDC	
		3.	JUSNL Backup SLDC- Backup ERLDC	
		4.	JUSNL Backup SLDC- DISCOM 1	
		5.	JUSNL Backup SLDC - DISCOM 2	
		6.	JUSNL Backup SLDC - DISCOM 3	
		7.	JUSNL Backup SLDC - DISCOM 4	
		8.	JUSNL Backup SLDC - DISCOM ..n	
		9.	With Other Applications (URTDSM/Renewable Energy Control Centres/IPPS)	
		10.	………..Any Other Association………..	

Vol. II, Part-A

APPENDIX-J

List of equipment for buy-back

List of equipment for buy-back (ERLDC)

S. No.	Item Description	Make/model/S.no. of equipment	Qty. Handed Over
1	SCADA Server/CFE	HP PROLIANT DL360P GEN8	2
2	ISR server	HP PROLIANT DL360P GEN8	2
3	SAN Box	HP	2
4	SAN Mgt Server	HP PROLIANT DL360P GEN8	2
5	Nas Box	HP	1
6	Tape Library	HP	1
7	ICCP Server	HP PROLIANT DL360P GEN8	2
8	NMS Server	HP PROLIANT DL360P GEN8	2
9	Workstation console with 23" display	FUJITSU	4
10	Lan Switch	HP	14
11	Laptop	DELL	2
12	Wan Router	CISCO 3945	7
13	Color Printer	HP	2
14	MFP Printer	RICOH	2
15	GPS	MASIBUS	1
16	Display Day	MASIBUS	1
17	Display Time	MASIBUS	1
18	Display Hz	MASIBUS	1
19	Display Abt	MASIBUS	1
20	Web Server	HP PROLIANT DL360P GEN8	2
21	Firewall	FORTIGATE 100D, CHECKPOINT 4200	4
22	CMC Console	DELL	1
23	DRS Server	HP PROLIANT DL360P GEN8	2
24	PDS Server	HP PROLIANT DL360P GEN8	1
25	PDS Console	FUJITSU	1
26	VPS Led	DELTA	27
27	DTS Server	HP PROLIANT DL360P GEN8	2
28	DTS Console	FUJITSU	4

29	Splitter	SAN TELEQUIP	100
30	Server Rack with KVM switch	MASTERVIEW MAX CS1315	4
31	Remote Console 23"	FUJITSU	2
32	Inkjet Printer	HP	4
33	Remote Router cum Firewall	CISCO 3945	4
34	Remote Console 55'	FUJITSU	6
35	Identity Server	HP PROLIANT DL360P GEN8	2
36	SMC workstation	DELL	1
37	U Type Work Stn Desks -I		4
38	Chairs		6
39	Fireproof Software storage	GODREJ	1
40	VCS MCU	POLYCOM	3
41	Video End Points	PROGILITY	3
42	HD camera	POLYCOM	4
43	Micophone Basestation	POLYCOM	3
44	Wireless Microphone	REVOLABS	6
45	Collar Microphones	REVOLABS	6
46	Lcd VDU Wall	DELTA	10
47	WALL ARRAY SPEAKERS	REVOLABS	3
48	AMPLIFIERS	CROWN	3
49	Terminal Server	SAN TELEQUIP	10
50	RTU Simulator	CTSIM	1
51	40 KVA UPS	DELTA	2
52	BATTERY BANK	Exide	2
53	UPS Control/Monitoring console	DELL	1
54	Input ACDB	VIDHYUT CONTROL PVT LTD	1
55	Output ACDB	VIDHYUT CONTROL PVT LTD	1
56	Spare Server	HP PROLIANT DL360P GEN9	2

List of equipment for buy-back (JUSNL)

S. No.	Item Description	Make/Model	Sl. no. of equipment
1	**Computer System Hardware**		
I.	SCADA/EMS Server	Dell Power Edge R610	38019284605
			25019056765
II.	ISR Server	Dell Power Edge R610	24958590589
			38079750781
III.	Communication front End (CFE)	Dell Power Edge R610	37958818429
			29372621437
IV.	ICCP Server	Dell Power Edge R610	27195839101
			20605025917
V.	NMS Server	Dell Power Edge R610	35842502269
			33665719933
VI.	workstation Console integrated with dual 19" monitor	Dell Precision T 1600	28869437773
			39150273997
			21287837773
			NA
VII.	Terminal Server for 40 Serial ports	Moxa Nport 6610-8	NA
2	**LAN Switch**		
I.	48 port L3-LAN Switch for SCADA/EMS LAN	Techroutes S3548	S31041096
			S31041098
II.	24 port L3-LAN Switchs for Web Server LAN & IT application LAN	Techroutes S3524	S34020155
			S34020153
			S34020149
			S34020146
III.	48 port L3-LAN Switch for SAN Switch		
IV.	24 port L3-LAN Switch for External DMZ LAN		

V.	24 port L3-LAN Switch for Server management LAN		
VI.	24 port L3-LAN Switch for ICCP LAN		
VII.	24 port L3-LAN Switch for Internal DMZ LAN		
VIII.	CFE 16 port LAN Switch	Techroutes S3548	S34020168
			S31041098
3	**Laptop for Maintenance**	Dell Vostro	14309179813
4	**WAN Routers**		
I.	WAN Routers at JSEB end	Techroutes TSR3800	RU800182
			RU800366
II.	WAN Routers (4X G.703 Ports configurable from 64 kbps to 2 Mbps LAN interface)	Techroutes TSR3800	RU800400
			RU800413
III.	WAN Routers (4X G.703 Ports configurable from 64 kbps to 2 Mbps, Dual LAN interface)	Techroutes TSR3800	RU800361
			RU800359
5	**Printers**		
I.	Colour Laser Printer	Xerox Phaser 7500	NA
II.	B/W Laser Printer	Xerox Work Centre	3246379547
			3246379440
6	**Time & Frequency System and external displays**		
I.	Time & Frequency System (GPS Based)	Sertel TGPS-300	NA
II.	Digital display for Day	Sertel	NA
III.	Digital display for Time	Sertel	NA
IV.	Digital display for Frequency	Sertel	NA
7	**Web System**		
I.	Web Servers	Dell Power Edge R610	20665492093
			4231283101
II.	External Firewall with NIPS	Watch Guard XTM8	80B7027F2-11A
			80B702818-A58D
III.	Internal Firewall with NIPS	Sophos UTM 220	A18053199EAEDE1
			A180539F107911B

IV.	Centralized Management console	Dell Power Edge R610	33726186109
V.	Data Replica Server	Dell Power Edge R610	35902968445
			27135372925
VI.	Wan Router cum firewall for Connectivity with ISP		
8	**PDS and RTU and ICCP integration testing system consisting of:**		
I.	PDS Server	Dell Power Edge R610	29312155261
II.	workstation		
III.	Wan Router cum firewall		
9	**Video Projection System**		
	Video Projection System for Control Room (4*2 Module, each 67" diagonal)	Delta	C7450FC22MB0171
10	**DTS Server**		
11	**Workstation (Training Console**		
12	**Remote Consoles with dual Monitor**		
I.	Remote Consoles with dual 24"inch Colour Monitor		
II.	Colour inkjet printer		
III.	Router cum Firewall		
13	**Remote Consoles with Single Monitor**		
I.	Remote Consoles with Single 19"inch TFT Monitor	HP Prodesk	INA441T7PM
			INA441T7SI
II.	Colour inkjet printer	Office Jet Pro 8000	CN15N3Q0TS
			CN15N3Q0SX
14	**Wall Mounted Remote Consoles**		
I.	Wall Mounted 55" Screen		
II.	CPU		
III.	Router		
15	**Storage System**		
I.	SAN Box		
II.	SAN Management Server		
III.	NAS Box		

IV.	Tape Libraries		
16	**Server Management Console**		
17	**Server Rack with IP based KVM Switch**		
18	**Furniture**		
I.	Chairs		
II.	Fireproof Software Storage box		
19	**Video Conferencing System**		
I.	Configuration Laptop with associated accessories		
II.	Video Endpoints		
III.	HD Camera		
IV.	Microphone Base Station		
V.	Wireless Microphones		
VI.	Collar Microphones		
VII.	LCD Video Walls		
VIII.	Wall Mounted Line Array Speakers		
IX.	Dual Channel Power with Software and all accessories		
20	**DTS Laptop with Software and all accessories**		
21	**Terminal Server System For 101 based RTU Terminal**		
I.	16 Ports Terminal Server		
II.	Panel with Accessories		
III.	24 Port LAN Switch for Terminal Server		
22	**Test Equipment for RTU**		
I.	Laptop PC for above software tools along with interfacing hardware		
23	**Auxiliary Power Supply**		
I.	40 kVA (32kw at 0.8pf) UPS running in Parallel	Delta	GES803HP33120 GE803HP35217
II.	VRLA type Battery banks for above UPS	HBL	NA
III.	Input ACDB (150kVA rating)	PCI	1018546C001
IV.	Output ACDB (100kVA Rating)	PCI	1018547D001

V.	125kVA DG Set	Jackson Limited	CJS-13120151
VI.	Accessories for Maintenance of VRLA type batteries	NA	NA
VII.	DC filter assembly	NA	NA
VIII.	Input AC filter assembly	NA	NA
IX.	Output AC filter assembly	NA	NA
24	**Any other items (Mandatory Spares)**		
I.	Server (one of each type)	Dell Power Edge R610	42372849277
II.	Workstation Console with Dual Monitor	Del Predision T 1600	34167133261
III.	LAN switch (One of each Type)	Techroutes S3548/S3524	S31041097 & S34020170
IV.	WAN Routers (One of each type)	Techroutes TSR 3800	RU800406
25	**VPS (Mandatory Spares)**		
I.	Video Proection System consisting of one module of 67" screen, one video projector, one controler and all associated hardware	Delta	NA
II.	Each type of power supply module of projection system	Delta	NA
III.	Each type of cooling fan assembly of projection system	Delta	NA
IV.	Dust filters	NA	NA
V.	Video projection system Lamps	Delta	NA
VI.	Time and frequency system (GPS based) without antenna	Sertl TGPS-300	NA

Note: The above list is tentative and the list for remaining RLDC/SLDCs shall be shared during detail engineering.

Vol. II, Part-A
Appendix-K
Vendor Taking

----- FORMAT TO BE FILLED BY Contractor ----

Document No:

Name of the Owner

Subject:

1. This is to Certify that the Hardware and Software being offered as part of the contract does not contain embedded malicious code that would activate procedures to:

   (a) Inhibit the desired and designed function of the equipment.

   (b) Cause damage or corruption [includes physical / software / data] of or to the user or equipment by way of malicious exploit.

   (c) Tap information resident or transient in the equipment / networks.

2. The contractor will be considered to be in breach of the contract, in case physical damage, corruption or loss of software / data or infringements related to copyright and Intellectual Property Rights (IPRs) are caused due to activation of any such malicious code in embedded software.

(Authorised Signatory)

Name/ Designation/ Address of the firm

Seal of the firm

Date:

Place:

---- TO BE FILLED BY Contractor REPRESENTATIVE AT SITE DURING COMMISSIONING / MAINTENANCE ----

DECLARATION OF CONFIDENTIALITY

I acknowledge that, in my capacity as a member (or staff, employee) of M/s ...., I will have access to certain Confidential Information (as defined in Agreement between Owner and M/s ....) of Owner, which may be in oral, written or any other form.

I understand that all ______________ members must sign a Declaration of Non-Disclosure when they commence their association with the ____________. Under this declaration, members consent to keep all matters to which they are privy related to all projects being conducted at the _________ confidential.

I agree that during my association with the Project relating to Owner and after the competition/termination of Project, I shall not disclose to any other person, firm or corporation, any confidential information relating to Owner's Company.

I also understand that I am required to notify .... of the _____________ or his/her designate immediately of any breach of my obligations or conflict of interest under this agreement which comes to my attention.

By signing and returning a copy of this document, I confirm my understanding and acceptance of the above clause and will comply with these clauses. I also agree that my obligation to comply with the above will survive my termination of association with the M/s ___________ in future.

Contractor Representative Signed: ______________________________

Contractor Representative Name (printed): ______________________________

Contractor Representative Employee ID: ______________________________

Sign and Name of Owner's Executive as Witness: ____________________

Date: __________

PART B

INTRODUCTION

PART B: INTRODUCTION

Introduction

This Part B of Volume-II describes the technical specifications for SCADA/EMS System, tobe procured as a part of this Project. The description includes requirements in respect of Control Center computer hardware and software, SCADA/EMS functions, user interface,testing, maintenance etc. The supplier of the system shall ensure that support services formaintenance are also available even after the maintenance period.

Proposed System

The SCADA/EMS system shall establish modern computer and control system at Main &Backup Control Centre. The technical requirements for various functions of SCADA/EMS system are described in subsequent sections.

The Bidders are encouraged to offer their standard products that meet or exceed the specification requirements. However, the proposal will be judged by its conformance to theSpecification. These products may be provided from their in-house baseline offerings, thecomputer manufacturer and established third-party software suppliers. The proposal shallclearly identify all deviations from the Specification to help Employer/Owner evaluate the degree of conformance of the Bidder's offering.

The System Design Parameters and Performance requirements for SCADA/EMS systemare specified in **Part B Appendices C & D**.

All the variable parameters of SCADA/EMS System, which require adjustment from time-to-time, shall be defined in the database and shall be adjustable by system users throughgraphic user interface displays. All periodicities and time intervals contained in the Specification that define these parameters shall be considered as initial values to be used for performance purposes. The adjustments made to parameters by the dispatcher or theprogrammer shall become effective without having to reassemble or recompile programs.

The specific requirements for output results are described along with the other requirements of each function. However, all results shall be stored in a form accessible fordisplay and printing, whether or not explicitly specified in the particular subsection. The application result storage details shall be submitted during detail design stage. The systemshall be designed such that failure of single server or single peripheral device shall not render the system unavailable.

Critical & Non-Critical functions

SCADA/EMS System functions are classified as Critical or Non-critical function. At control centre every critical function must be supported by sufficient hardware and software redundancy to ensure that no single hardware failure will interrupt the availability of the functions for a period exceeding the failover time defined in the specification.

Non-critical function may not be supported by hardware redundancy and can be suspendedin case of non-availability of corresponding hardware.

i) The following functions are classified as Critical functions:

a) SCADA System Functions

b) EMS functions

c) FEP and ICCP System

d) AGC Functions

e) Dynamic security Assessment (DSA) (wherever applicable).

f) Historian and Reporting system

g) User Interface Requirements

h) Network Management system

i) Web and Scheduling Applications

j) Cyber Security System

k) Dispatcher Training simulation (DTS) (wherever applicable)

ii) The following functions are classified as Non-Critical functions:

a) Database modification and generation.

b) Display modification and generation.

c) Report modification and creation.

d) Software configuration and system generation.

e) Antivirus and Patch Management.

f) VAPT function.

g) Document Management System

h) Centralized Management System

i) OPC Server

j) SIEM

k) Anti-APT Server

Organization of PART-B of the specification

Sections 1 through 9 and Appendices provide the requirements for SCADA/EMS system to be procured for this project as follows:

SECTIONS

SECTION 1: SCADA SYSTEM FUNCTIONS

SECTION 2: EMS FUNCTIONS

SECTION 3: USER INTERFACE REQUIREMENTS

SECTION 4: SYSTEM SOFTWARE REQUIREMENTS

SECTION 5: HARDWARE REQUIREMENTS

SECTION 6: CONFIGURATION CHARACTERISTICS

SECTION 7: INSPECTION &TESTING

SECTION 8: WEB AND SCHEDULING APPLICATIONS

SECTION 9: CYBER SECURITY REQUIREMENTS

APPENDICES

APPENDIX A GLOSSARY

APPENDIX B SAMPLE REPORTS & DISPLAY FORMATS

--End of the Section--------------------------------

Section 1

SCADA System Functions

Table of Contents

Section 1 SCADA System Functions

1.0. Introduction

This section describes the functions to be performed by the SCADA/EMS system being procured. The applications of SCADA system are broadly grouped into the followings:

a) SCADA Applications

b) Information Storage & Retrieval (HISTORIAN)/ Historian System

1.1. SCADA Functions

The following SCADA functions are envisaged under this specification.

a) Data Acquisition from any data communication device in substation any device i.e., Remote Terminal Unit (RTU), Sub-Station Automation System, Gateway, Data Concentrator cum Protocol Convertor (DCPC), Phasor Data Concentrator etc. communicating with Control Centre SCADA system on IEC 60870-5-101, IEC 60870-5-104 protocol and Secure IEC 60870-5-104 protocol). Supplied Solution shall support secure IEC 60870-5-104.

b) Data Exchange with Control Centers

c) Data Exchange with URTDSM, REMC, MODBUS RTU, MODBUS TCP/IP, OPC

d) Data Exchange with Historian system

e) Data exchange through Web Services

f) Data exchange with scheduling application WBES

g) Data exchange with all other application

h) Data Processing

i) Network Status Processor

j) Sequence of Event Recording

k) Supervisory Control

l) Visualization application

1.1.1 Data Acquisition

Real-time data shall be collected from field devices located at various Substations and Power Plants on IEC 60870-5-101, IEC 60870-5-104 protocol. The data includes analog, status and SOE inputs. The capability to collect other data in the future, such as momentary change detection inputs, phase angle, wind speed, wind direction, temperature, rainfall, humidity etc. shall be provided. In addition, RTU data acquisition shall be capable of supporting all possible user-declarable RTU operating modes (e.g., up/down, in scan/out-of-scan and test).

The SCADA system shall be provided with the IEC 60870-5-104 protocol and IEC 60870-5-101 protocol and Secure IEC 60870-5-104 protocol. The SCADA System shall be provided with all security provisions as per IEC 62351 Standard. The bidder shall fill and submit the protocol implementation conformance statement in line with the IEC 62351 Standard attached at Appendix J along with the bid documents.

The Control Center shall support all features of the IEC 60870- 5-104 and the IEC 60870-5-101 unbalanced protocol. In case field device supports Secure IEC 60870-5-104 protocol, same shall be integrated in secure mode at control centre end.

All the functions for RTU data acquisition as described in the sub-sections below shall be implemented for existing RTUs. Feature shall be available in SCADA System to accumulate data for a user defined time period (i.e.,15-minutes,1-day,1-week,1-month) and it shall be automatically reset the same after user defined time.

All the RTUs will be reporting to Main Control Centre and Back up Control Centre directly. Typical architecture of RTU data reporting to Main and Back up Control Centre is given in **Appendix-F.**

1.1.1.1 Periodic Scans

Status data shall be reported by exception from the field device (RTU, MFT etc and shall be updated and displayed within 2 seconds if communication is through Fiber Optic otherwise within 4 seconds at the first level Control Centre in worst case. A complete scan of all status data from the RTU shall be made every 10 minutes and any discrepancies between field status and Control Centre database shall be reported by an alarm message.

Analog data shall be periodically updated at Control Centre from field devices. Periodicity of data acquisition shall be user configurable, initially 2 seconds and up to 30 seconds. Analog data shall also be reported by exception (spontaneously) from field device when its value changes from its previous value by more than 20% (user configurable) and shall be updated at the control centre within 5 seconds.

The SCADA should have capability to take time tag analog and status information.

1.1.1.2 Demand Scans

The Control Centre computer system shall be able to collect any and all analog and all status values (individually, as scan groups, or collectively) from any of its field devices on a non-periodic (demand) basis.

A UI showing following times shall be available:

- Pooling time or poll request (i.e., time on which request is sent to RTU) shall be available of all points (Analog, Digital etc.) in real time.
- Last data updation time or response received time (i.e., time in which data are received/updated at control centre from RTU) in real time.

A UI with demand scan button to be provided for retrieving values from RTU. Demand scans shall be initiated automatically for an RTU whenever the following situations arise:

a) A change of status of RTU is detected
b) After completion of a successful supervisory control action
c) Periodically as per user defined interval
d) Link Initialization.
e) Upon request by a User

1.1.1.3 Backup Communication Channel Processing

Redundant communication channels will be provided between SCADA/EMS System (Control Centre) and RTUs. If valid data cannot be acquired from one of the RTUs, the Control Centre System shall automatically failover to the backup Communication channel. A communications failure shall not cause a server failover.

The backup communications channel shall be tested periodically up to RTU, without manual intervention, to determine its readiness to take over upon failure of the primary channel. An alarm shall be generated for any backup channel that is not ready to take over. A display shall be provided that shows whether each RTU is being scanned on the primary or backup communications channel. The user, via this display, shall be able to:-

a) Force scanning to a specific channel (primary or backup)
b) Manually fail a channel
c) Inhibit automatic failover of communications
d) Inhibit automatic fail-back of communications

1.1.1.4 RTU in Test Mode

A User of a Control Centre computer system shall be able to declare that any associated RTU is in the test mode. Placing an RTU in test mode shall generate an appropriate event message. When an RTU is in the test mode, the real-time database shall retain the last value from all points collected via the RTU before it was placed in the test mode. The points of RTU in test mode shall be marked with a quality code in the database indicating that their source RTU is in the test mode. All system displays, programs, data links, and other devices shall use this value.

Supervisory control through RTUs that are in the test mode shall not be permitted.

When an RTU is removed from the test mode, an event message shall be generated, the test mode quality code shall be removed from all points assigned to the RTU, the database values shall resume updating on each scan and any controls for the RTU shall be enabled.

Test displays shall be provided that show the actual values being received from the RTU in the test mode. When an RTU is in the Test mode, test personnel shall be able to inhibit and re- enable telemetry failure logic for the test RTU. When failure logic processing is inhibited, the RTU shall be scanned at the scheduled times regardless of whether the RTU responds correctly, sends an incorrect reply, or fails to respond.

A time-ordered record of the last 100 communications errors shall be maintained for each RTU in the test mode and shall be available for display. Telemetry failure processing shall be automatically resumed when the RTU is taken out of the test mode. It shall be possible for a Control Centre to have up to five (05) RTUs in the test mode simultaneously. RTU test mode can be assigned by selecting either RTU or entire points of the station.

1.1.1.5 Telemetry Failure and Delete from Scan

If valid data is not received from an RTU in response to a scan command, another scan request for data from that RTU shall be issued. If valid data is not received from an RTU after configurable number of retries, each point affected shall be marked with a telemetry failure quality code and an alarm shall be generated. If an entire RTU or its communication channel fails, only a single alarm shall be generated and the RTU shall be marked with telemetry failure quality code. Communication with this failed RTU shall be retried at a periodicity, specified by the user, which shall be different from the normal periodic scan rate of the RTU.

In the event of telemetry failure, the last good value or status shall be retained in the database for each affected point. The user shall be able to substitute a value in the database for any point that is experiencing telemetry failure. When telemetry returns to normal, the Control Centre computer system shall automatically resume updating the database with the scanned data. No manual entry enabling should be required when data is not coming from RTU

The user shall be prohibited from entering a value for a point, without putting the sameout of scan while the telemetry from that point is in scan. The user shall be able to delete any point (or entire RTU) from scan processing and substitute a value (or values) for the data. Such points shall be marked with a delete-from-scan quality codeand, as may be necessary, a manual entry quality code. When the user restores a point or RTU to scan processing, the Control Centre computer system shall automatically resume updating the database with the scanned data. User action for scan deletion and restoration shall generate an appropriate event message. Delete from scan shall also apply to Control Centre calculated points, in which case the term scan processing shall encompass the calculation of these values.

1.1.1.6 RTU Time Synchronization

The Control Centre computer system shall synchronize the time in the RTUs using the time synchronization function as per the IEC 60870-5-101 and 104 protocol standards periodically. The Control Centre computer system shall dynamically acquire and calculate the time of delay in propagation of a message to each RTU (Dynamic delay acquisition) and shall adjust the time synchronization process for this propagation delay wherever IEC 60870-5-101/104 Protocol is being implemented.

1.1.1.7 RTU Communication Monitoring, Recording and Statistics

The SCADA system shall be capable of monitoring and recording the data exchange that is occurring between the SCADA system and the RTU without affecting the normal RTU data acquisition process. This shall include details such as the bytes exchanged, interpretation of type of data (ASDU), interpretation of the message as per the communication protocol and the time stamp at which the message exchange took place. A User shall be able to invoke the monitoring and recording of the data exchange between the SCADA system and the RTU for at least five RTUs simultaneously.

For IEC-60870-5-101, IEC-60870-5-104 and all standard protocols it shall be possible to trace the protocol telegram and display it for the operator in a User Interface in interpreted view and HEX view.

The SCADA system shall also maintain the RTU communication statistics for a period of one month, **on daily basis,** on hourly basis **and any user defined periodicity** for all RTUs. The details to be maintained in statistics are 'Number of poll requests sent by the SCADA system', 'Number of responses received from the RTU', 'Number of no reply errors (Communication channel failure, RTU device failure)' and 'Number of faulty packets' received. The RTU communication statistics shall also be transferred to Historian System. **The status of primary and secondary channel availability and data operation on it must also be stored in the historian.**

The SCADA system shall also maintain the latency of data received from RTU to control center. Real time RTU status and RTU's availability report **shall also be available/ exportable** in text or CSV or Excel file from system **as and when required/periodically** in SCADA system.

CFE requirement: CFE server should be able to operate in listening mode (able to receive signal without request)

1.2 Data Exchange

1.2.1 Data Exchange with Control Centres

The following ICCP blocks shall be implemented in the supplied SCADA/EMS system

a) Block 1 (periodic data transfer)

b) Block 2 (exception-based data transfer)

c) Block 4 (information messages)

d) Block 5 (controls)

All the Digital/status points specified in **Appendix-F** shall be modeled as controllable points using ICCP protocol.

The SCADA/EMS system shall acquire Real-time data like analog, status, calculated, manually entered and time stamped SOE data from connected control centre over Secure Inter Control Centre Protocol (ICCP) protocol.

The communication protocol between the Main and Backup Control Centre can be a proprietary protocol ensuring cyber security as per latest guideline or secure mode ICCP protocol and to DISCOM on ICCP Protocol. The bidder shall submit the ICCP PICS table and Secure Protocol Implementation conformance statement along with the bid.

System shall support Integration of Main and Back up Control Centers with **other** Control Centers on secure mode ICCP protocol.

The required communications links shall be provided by the Owner for data exchange among Control Centers. The communications links for data exchange among control centres shall allow configuration of each channel transmission rate up to 2 Mbps or more. Communication links shall be configured as Main (or Primary) & Backup (or Secondary) links. The communication links shall be designed for automatic switchover to backup communication links on failure of main links.

The backup communications channel shall be tested periodically, without manual intervention, to determine its readiness to take over upon failure of the primary channel. An alarm shall be generated for any backup channel that is not ready to take over.

All the performance requirements for data exchange with control centres are required to be met with availability of communication links. Status data (Value, Quality Code and Time Stamp along with milliseconds accuracy) shall be reported periodically & by exception from respective Control Centres and shall be updated in the database & displayed at the operator consoles within 2 seconds of receipt at ICCP servers. A complete scan of all status data shall also be made every 10 minutes as an Integrity Check and any discrepancies between databases of Control Centres shall be reported by an alarm message to the operator.

Analog data (Value and Quality Code) shall be periodically exchanged at a periodicity of 5 seconds. This periodicity shall be set by the ICCP client as per the ICCP protocol. This analog data shall be updated in database & displayed at the operator consoles within 2 seconds of receipt at ICCP servers. All scans shall be monitored and any failure to shall be alarmed. The computer systems at Control Centre shall be able to exchange various types of data within the delivery times and response times listed in **Appendix C & D**.

Automatic resetting of ICCP stack modules should be done whenever there is failure of communication channel.

The contractor shall provide user friendly ICCP configuration interface. The ICCP communication application shall have detailed logging of all the activities on a communication link including communication statistic of connectivity with other SCADA system.

The logs shall be organized in multiple levels such as operator controls, error messages, warning messages, event messages and low level tracing. These logs shall also be transferred to Historian system and should be available preferably area-wise, station-wise & discom-wise etc.

The SCADA system shall also maintain the communication statistics for Telemetered data for a period of one month on hourly basis for all control Centers. The communication statistics shall also be transferred to the Historian system. Based on these statistics; operator should be able to generate the reports of availability of communication link in percentage.

The operator shall also be able to generate the report of availability of ICCP link. The sample format is attached at **Appendix-B**.

The SCADA system shall be capable of monitoring and recording the data exchange that is occurring between the systems across all Control Centers without affecting the normal data acquisition process.

Main and Back up Control Centre of RLDC & SLDCs will exchange data through ICCP as per typical architecture given in **Part-A, Appendix F_ICCP, RTU and Historian Configuration.**

1.2.2 Data Exchange with Historian System

The SCADA/EMS system (consist of any database point/field of SCADA, ICCP, EMS, DSA, AGC etc.) shall be able to exchange data with Historian system directly by assigning their database field unique ID for all type of data envisaged in the specification including State Estimator values & other EMS Applications with associated performance parameters.

1.2.3 Data Exchange with Other Systems & Third-party applications

The SCADA system shall provide web services on SOAP and REST API that allow multiple applications to exchange (bi-directional) any data points (real time, future values like various forecasts/schedules) including alarms and events. The SCADA system shall provide web services that allow multiple applications to exchange any real time data points & vice-versa including alarms and events in secure manner ensuring latest cyber security guideline from statutory authority.

Data transfer from SCADA to IT/Any Other network should be made through secure services such as API calls. As per the requirement of the User, the Contractor shall incorporate new APIs in the SCADA System during AMC period also. If required, the APIs should be modified in such a way that, the corresponding data can only be accessed using API Keys.

The functionality of Web Services is explained in **Section 8 (Section describing web services)** in detail.

SCADA System shall have inbuilt OPC-UA Server and client functionality. OPC Client shall be able to interact with SCADA server using a defined OPC-UA interface. The SCADA system shall also have an ODBC (Open Database Connectivity) interface which shall allow all the real-time data to be accessible by Personal Computers (PCs) running Microsoft-Windows based applications.

The value and the quality code of the real-time data shall at least be accessible through this interface. The SCADA system shall have the facility to integrate the data from spread sheet applications, XML, JSON and .csv files etc into real-time database & vice-versa. The time stamp, value and the quality code of the real-time data shall be accessible through this interface. Limitation if any or pre-requisite on PC for use of this interface shall be clearly defined in the bid.

The proposal shall clearly mention the platform and product limitation if any for the above functionality. The SCADA system shall have the facility to exchange the data (incl. value, time-stamp and quality code) with all these formats. JSON, .XML and spreadsheet applications .CSV files into real-time database and vice-versa.

Further, The SCADA system shall also be capable to exchange the data on IEC-104.

1.2.4 Data Exchange with Market Applications and Open Access

The SCADA system shall acquire data from Market applications and put in SCADA database for visualization, archival in Historian, trending, playback and all other purposes in secure manner ensuring latest cyber security guidelines from statutory authority. SCADA vendor has to develop API as per requirements, for integration of following data:

- Short term transactions in trade (Bilateral and Power exchange)
- Scheduling data
- ATC (Available Transmission Capacity) and TTC (Total Transmission Capacity)
- Market Clearing Price (area-wise)
- Market Clearing volume (area-wise)
- Deviation Settlement Mechanism Price (DSM)

All data mentioned in the above bulleted points would be available in one or more of the following formats shall be finalized during detail engineering– **Dedicated API, SOAP/REST and OPC etc.**

All the data exchange to/from SCADA system shall be in secure manner ensuring latest cyber security guidelines from statutory authority throughout the period of contract considering all the amendments.

1.2.5 Data Exchange with Modbus

The SCADA system shall have the functionality of data exchange using MODBUS, which includes Modbus TCP/IP, OPC and Modbus RTU protocol to integrate local devices like weather sensors, UPS, rooftop solar etc.

1.3 Data Processing

The SCADA system shall prepare all the acquired data for use by the power system applications. The SCADA system shall have capability to accept data from the following sources:

a) Real-time (also referred as telemetered) data received from control Centers (i.e. ICCP data) and RTUs
b) Calculation
c) Manual entry
d) Sequence of events data from RTUs and connected control centers (over ICCP and exchange of SoE files)
e) EMS applications
f) Stored data
g) Offline Applications
h) URTDSM/REMC/Any other Web Based Applications etc.,
i) Any other external source

The data processing requirements shall apply to data collected from all specified sources. All time stamp used for data shall be in IST. Wherever source data reported in any other time format, it shall be converted to IST. All input data and parameters, whether collected automatically or entered by a user, shall be checked for reasonability and shall be rejected/flagged if they are unreasonable but its value should be available in database for monitoring by user.

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 all computer systems shall continue to operate with the old data or manually replaced data in the presence of unreasonable data.

1.3.1 Analog Data Processing

Analog data shall be stored in engineering values in SCADA database & processing shall be performed according to the requirements listed below.

a) Reasonability Limit Check

The reasonability limits shall represent the extremes of valid measurements for the point's value. All analog values shall be compared against defined high and low reasonability limits. The comparisons shall be performed at the scan rates of the analog values. An alarm shall be generated the first time a reasonability limit violation is detected.

The last valid value of the variable shall be maintained in the database and marked with a quality code indicating the *'reasonability limit violation'*. When data returns to a reasonable value, the new value shall be accepted, and return-to-normal message/events shall be generated. Reasonability limits shall be adjustable by user and in case of restart/ database update values should be retained with in database.

b) Zero dead band processing

All analog values shall be processed for *'zero dead band processing'* to nullify inaccuracies in the transducers output when the actual process value is *'zero'*. If the acquired value falls between the specified dead band range around *'zero'* then the processed value shall be clamped to zero else the actual value shall be considered for database and display purpose. There shall be configuration setting at global and individual point level.

c) Limit Monitoring

For bi-directional quantities (positive or negative) there shall be a set of three limits for each direction. For unidirectional quantities there shall be a set of three limits in one direction. These limits will represent increasing levels of concern and shall be named as **"Operational"**, **"Alarm"** and **"Emergency"** limits.

These three limits shall be set within the boundaries of reasonability limit. All acquired and calculated analog point shall be compared against above sets of high and low limits each time the value is scanned or calculated. Whenever a monitored point crosses a limit in the undesirable direction a limit violation alarm message shall be generated. The alarm message shall include:

- Time of limit violation detection
- Station name
- Point name
- Point value
- Name of limit crossed
- Value of limit crossed

Whenever a monitored point crosses a limit in the desirable direction, an exit event message shall be generated. The exit event message shall contain the same information as a limit alarm message except that it indicates that the alarm region bounded by the limit that was crossed has been exited. If multiple limits have been crossed since the last check, highest limit crossed shall be reported. All limit monitoring shall preclude annunciation of multiple alarms when a value oscillates about an alarm limit by utilizing adjustable alarm dead-band for each point. It shall not be necessary to specify zero or infinity as an operational or emergency limit. Limit comparison shall be carried out only with respect to the specified limits.

The user shall be able to temporarily override an in-use limit by entering a new value. When the user overrides a limit, it shall be marked with an override flag in the limits display.

The override value shall be recognized, and any display, report, or logcontaining the value of the overridden limit shall include it as such. An override value shall be used instead of the permanent value until the user removes the override condition, selects an alternative limit set, or the system is re-initialized.

A limit override summary shall be provided that lists all overridden limits. Any change in alarm states resulting from a change in limit value shall be reported/ alarmed.

d) Sign conventions

The following sign conventions for the display, data entry and reporting of active and reactive power flow shall be used universally by all SCADA/EMS functions:-

With respect to bus bars, all imports to bus bars shall be represented with -ve sign and all exports from bus bars shall be with +ve sign. However, in case of generator the sign convention shall be reverse.

Equipment	Flow Convention

Bus	**Real power into bus:** Negative **Reactive power:** same as real power
Generator Transformer (Measurement on HV side)	**Real power low to high side:** Negative **Reactive power:** same as real power
Generator Transformer (Measurement on LV side)	**Real power low to high side:** Positive **Reactive power:** same as real power
Substation/Distribution Transformer (Measurement on HV side)	**Real power high to low side:** Positive **Reactive power:** same as real power
Substation/Distribution Transformer (Measurement on LV side)	**Real power high to low side:** Negative **Reactive power:** same as real power
Generator	**Real power out of generator:** Positive **Reactive power out of generator:** Positive
Reactors/Capacitors	**Reactive power into equipment:** Positive
Loads	**Real power into load:** Positive **Reactive power into equipment:** Positive

e) Data Validity Tests

Data validity tests shall be performed automatically (without data entry) at different voltage level and shall generate an alarm when data changes from valid to invalid. A return-to-normal message shall be generated when the data again becomes valid. The tests shall be performed as follows:

- The algebraic sums of telemetered, calculated, and/or manually entered MW and MVAr values for devices connected to a bus shall be compared to a tolerance, provided values are available for all such devices. In case of transformers values at primary/secondary require to be maintained by calculation from either of its sides if not available. Line reactors values should not be considered for MVAr sum of station.
- The MW and MVAr flows for switching devices that are open shall be compared to a tolerance.
- Redundant MW and MVAr flows for both ends of a branch shall be compared for differences greater than a tolerance.
- Redundant bus voltages at same system shall be compared for differences greater than a tolerance.
- Redundant frequency values (for the same electrical island/system) shall be comparedfor differences greater than a tolerance.

The system-wide tolerances shall be configurable by operator through a display. When invalid data is detected it shall be marked in the database with a quality code to denote the data is questionable. A data validity summary display shall be provided that lists all the invalid/questionable data and shall be reflected in alarm summary display for the violated condition.

f) Freeze data/Stale Data Check

SCADA system shall be able to detect Stale data/Freeze data which is not changing and SCADA quality is good for a pre-defined period (1 minute to 30 minutes) which is user-configurable (locally and globally). The freeze data check function shall represent the value, which is not changing/updating for a pre-defined time-period (user configurable).

An alarm shall be generated when freeze data is detected and when data returns to actual/normal value. A separate display for Stale data points shall also be available. A summary display shall be provided that lists all the freeze data for real-time as well as calculated values. Option of check/uncheck shall be user configurable for selecting the points for monitoring freeze data. In case of freeze/stale data, **freeze/stale data quality flag** should be assigned on the point/field and accordingly data should be switched between multiple sources as per the alternate data configuration methodology. Alternate Data Source should be activated. Separate display should be provided for summary of Stale Data.

g) Flat-Line check

SCADA system shall be able to detect flat line for calculated data which is not changing for a pre-defined period (1 minute to 30 minutes), which is user-configurable (locally and globally). There shall be alarm generation when flat-line value is detected and return to normal on correction of data. SCADA quality (Flat-line flag) should be assigned on the point/field and accordingly data should be switched to data from Backup control centre if Flat-line flag is not set at Backup.

1.3.2 Digital Status Input Data Processing

Each state of a digital input point represents the state of an actual device. The following digital input data types (as a minimum) shall be accommodated as per IEC 60870-5-101/104 standard:

- Single point information
- Double point information

(a) Two-state points: The following pairs of state names shall be assignable:

- Open-Close
- Tripped-Closed

- Alarm-Normal
- On-Off

(a) **Three-state points:** Any of the state combinations listed in (a) above shall be supported with a third, typically, in-transit state which is the case for slow operating devices such as isolator. The programmer shall be able to designate any combination of "bits" in the data representation of each three-state point as an undefined state. The programmer shall also be able to designate the in-transit state as open or closed for use by various SCADA/EMS applications.

(b) **Four-state points:** Any of the state combinations listed in (a) and (b) above shallbe supported with a fourth, typically, faulty state which is the case for CB. The programmer shall be able to designate any combination of "bits" in the data representation of each four-state point as a faulty state. The programmer shall also be able to designate the faulty state as open or closed for use by various SCADA/EMS applications.

All un-commanded status changes shall be alarmed. The data transfer convention of status points shall be as per the table below:

Status Points	Device Status	Bits Codes (Digital)	Value Codes (Analog)	Bits Coding at Control Center 1	Status Interpretation at Control Center 1	Values transferred toother Control Center-2	Bits Coding at Control Center 2	Status Interpretation at Control Center 2
Double point status	BETWEEN	00	0	00	BETWEEN	0	00	BETWEEN
	OPEN	01	1	01	OPEN	1	01	OPEN
	CLOSE	10	2	10	CLOSE	2	10	CLOSE
	INVALID	11	3	11	INVALID	3	11	INVALID
Single point status	OPEN	0	0	0	OPEN	0	0	OPEN
	CLOSE	1	1	1	CLOSE	1	1	CLOSE

1.3.3 Calculated Data Processing

SCADA/EMS system shall be capable of performing the following calculations at the indicated rates and storing the result in the database as calculated data corresponding to same SCADA field/point and shall be available for display. This calculation output shall not be considered as additional SCADA field/point for system sizing.

The database variables to be used for arguments and themathematical, statistical and logical functions to be used as operations shall bedefinable interactively at a workstation by dispatcher as well as by the programmer using database creation and maintenance procedures. The calculations shall be executed either on an exception basis i.e., whenever the inputs of the calculation's changes or periodically. The periodicity of calculation shall be user modifiable.

The user interface and suitable API shall be provided to real time Calculations for SCADA Data as well as estimated Data. There shall be no limitation on number of calculations and arguments involved in each calculation, which shall be defined in the real-time calculations. The vendor has to ensure the working of API.

Calculated analog values shall use database points (of SCADA and EMS applications input & output points) as the arguments and combined mathematical, logical and statistical functions as the operators.

The functions such as addition, subtraction, multiplication, division, maximum value with time of occurrence, minimum value with time of occurrence, average value, count, square root, exponentiation, trigonometric functions, logarithms and other statistical functions, logical & comparative operators such as AND, OR, exclusive OR, NOT, Less Than, Greater Than, Less Than or EqualTo, Greater Than or Equal To, and Equal To etc. shall be provided.

Calculated status values shall use database points as arguments and combinational logical functions as operators that include the logical & comparative operators AND, inclusive OR, exclusive OR, NOT, Less Than, Greater Than, Less Than or Equal To, Greater Than or Equal To, and Equal To.
Suitable rules or operators (such as multi-level parentheses) shall be provided to indicate the sequence of operations in the calculation. Some of the calculations on telemetered and calculated analog points are defined below.

It shall also be provided for operator to see the formula used for a calculated value along with real time value and quality flag, from the any display where calculated value is appearing. Calculation shall not be stopped due to single garbage value, it shall not be considered in calculation and generate output with proper alarms/flag. In addition, calculation shall not be stopped in case one of the input is not reporting/not correct/garbage. A separate list of all garbage/un-initialize analog/points shall be made available in separate display.

A tool shall be provided for extracting the information regarding the points which are used in multiple calculations along with calculations name.

1.3.3.1 MVA Calculation

MVA values for all lines/loads and transformers shall be automatically assigned and calculated for each set of MW/MVAR as per the formula MVA = SQRT (MW^2

+ $MVAR^2$). The calculation shall be performed at the fastest scan rate of the component data.

1.3.3.2 MW and MVAR Integration

MW & MVAR values for all lines/loads, transformers and generators shall be individually integrated at their scan rates over each quarter of an hour for 96 blocks (or for each 5-minute time period, resulting in to 288 block) of the day to calculate active & reactive energy. User selectable option to be provided for 5 mins/15 mins/user defined time period integration.

The energy values calculated as per user-defined period (5 mins or 15 mins etc.) shall be summed for each hour to compute hourly energy quantities. In line with integration of MW and MVAR, feature shall be available to integrate current also.

1.3.3.3 Rate of Change

The rate of change of variables shall be automatically calculated for each analog data using the following formula that filters the rate of change via exponential smoothing:

NewRate = A * OldRate + (1 - A) (NewValue - OldValue)/Time Interval

New Value and Old Value refer to the selected variable, A is a user-specified constant between 0 and 1, and Time Interval is the applicable scan rate as minimum and goes up to any user defined time (in secs).

The rate of change shall be compared to a threshold limit exceeding which an ALARM shall be generated. Such rate of change values shall be one of the fields associated with the corresponding analog data and shall not be a separately defined analog point.

The rate of change of variables tag shall be automatically associated with every data (analog values) field. Separate limits (in percentage and value) shall be associated for rate of change values associated with analogs and rate-of-change shall be user configurable (individual-analog-pointwise and bulk-analog-pointwise).

1.3.3.4 Average Value Calculations

For calculation of the average value of an analog points (all lines, loads, generators and transformers), the sampling frequencies of the point shall be same as scan rate and the time periods duration of interest shall be defined by the user.

Average of value over duration of interest = Sum of values of samples/No. of samples

The duration of interest shall be configurable on a system wide basis from 5 minutes to **60 minutes** in steps of 5 minutes (total 12 options to be provided for user's duration of interest). The results shall bear the time-tag of the time at the start of the interval. These calculations shall use the real-time clock. Initial setting for capacity and performance shall be 15 minute and it should be available to operator for last 24 hours.

Such Average values shall be one of the fields associated with the corresponding analog data and shall not be a separately defined analog point moreover, these average values shall be displayed in tabular form along with real-time values.

1.3.3.5 Max. and Min. Value Calculations

For calculation of the max/min value of an analog point (all lines, loads, generators and transformers), the time period (duration) of interest shall be defined by the user and max/min value shall be identified/calculated from all samples collected during the duration of interest.

The duration of interest shall be configurable on a system wide basis from 5 to 60 minutes in steps of 5 minutes. The results shall bear the time tag of the time at which the Maxima and Minima occurred. These calculations shall use the real-time clock and initially shall be performed for 15-minute intervals and it should be available to operator for last **24 hours**.

The ability to calculate and display the Maxima and Minima values of user-selected telemetered and calculated analog points shall be provided. The user shall be able to enter the point names and the duration (period) of interest.

Such Max. and Min. values shall be among one of the fields associated with the corresponding analog data and shall not be a separately defined analog point moreover, these maximum/minimum values with time shall be displayed in tabular form along with real-time values.

1.3.3.6 Insertion of forecasted data values in SCADA tags

SCADA system shall be provided with an UI interface/API to insert forecasted & scheduled values (one point & bulk both) for a defined time duration. These forecasted & scheduled values should be overwritten by recurring revisions with its revision number, in SCADA. Functionality of trending and comparison of forecasted & scheduled & present values shall be available on a single trend window. The insertion of forecast values shall be done automatically as and when future value of that point is available

1.3.3.7 System Load and Interchange data

The MW & MVAR flow and net interchange (both import and export) for each entity /area/licenses shall be calculated automatically, at prevailing scan rates. Calculation of these parameters shall be defined based on area and company.

1.3.3.8 Line and Transformer Loss Calculations

Line and transformer active and reactive power losses shall be computed for all lines and transformers where adequate data is available to permit such computations. Examples of adequacy are:

a) Active power flow measurements at both ends are available for active power loss calculations

b) Active and reactive power flow and voltage measurements at one end are available and computations shall include the parameters of the line and transformer models, such as resistance, reactance, susceptance, and transformer tap position.

1.3.3.10 Power Factor Calculation

PF values for all lines/loads and generator's transformer LV side shall be calculated as per the formula PF=MW/MVA. The calculation shall be performed at the fastest scan rate of the component data.

1.3.3.11 Data Availability Reports

Statistical Analysis for Availability of data: Communication Monitoring, Recording and Statistics- The availability of telemetered data shall be recorded viz. Period of availability/non-availability, number/percent of successful data updates, for a set of data source of individual data source and its reporting based on various filters such as area-wise, station-wise, region-wise, discom-wise, voltage level-wise, element-wise, etc.

Statistics of availability of data must be available in real time basis and also in the historian. Based on this statistic, operator should be able to generate the reports of availability of data in % terms station wise as well as region wise. A sample report is attached in Appendix –B.

1.3.4 Quality Codes

Quality codes indicate the presence of one or more factors that affect the validity of a data value. All quality codes that apply to a data value shall be maintained in the database for that data value.

For calculated data, the presence of a quality code on any of the component data values shall not disrupt the calculation using that value. The quality of the calculated value shall be the quality of its "poorest" component. Results of calculations that are manually overridden by the user shall be denoted with a quality code that can be differentiated from the propagation of a manual entry quality code from one of its component values.

The following are the data quality codes that have been defined in this Specification and whether the quality code should propagate to the result of a calculation.

S. No.	Quality Code	Propagate	Details
1	Telemetry Failure	Yes	Telemetry has failed
2	Delete from Scan	Yes	User has disabled the update of data from database
3	Reasonability Limit Exceeded	Yes	Reasonability limit violated
4	Questionable/In valid	Yes	When the data is questionable as mentioned in sectionregarding 'Data Validity Test'
5	Manual Entry	Yes	Values entered Manually
6	Manual entry at remote end	Yes	Values entered Manually at remote end
7	Alarm Inhibit	No	Alarm processing has been prohibited
8	Not in service	Yes	Point is temporarily removed from service
9	Alternate/Redundant Data Source	Yes	Data Quality code indicating alternate source of data
10	State Estimator Replaced	Yes	Replaced by corresponding State Estimator output
11	Alarm Limit flags	Yes	Which Alarm limit is exceeded (out of 3 or more defined
12	Suspect Data	Yes	Data is "Suspect" quality by probable reasons
13	Uninitialized	Yes	Data has not been initialized even once
14	Good Data	Yes	Data is available with "Good" quality
15	Freeze/Stale Data	Yes	Data is not updating but the quality is "Good"
16	Flat line	Yes	Calculated points not updating

NOTE: Above quality codes shall be identified in SCADA with one or multiple identifiers.

1.3.5 Real-time Data Storage and Playback

All real-time data (Analog and status) shall be continuously available online for at least one (01) year at scan rate for the trending, reporting and playback. Data older than one (01) year shall be automatically archived and shall be accessible for playback if required by owner.

It shall be possible to playback above stored data on Single Line Diagram and Network Diagram for a configurable time window (configurable from data scan rate to any user selectable time) by defining Start time & Date, End date, time of window , playback rate and sampling rate for play back, faster and/or slower playing. The user shall be able to playback data on all type of displays, dashboard defined by user. Option of different concurrent sessions shall be available for playback for users. It shall also be possible to set a different sampling rate for playback than the sampling rate for data storage. It shall be possible to have tabular and graphical trends from the stored data. The trending of graphs from the displays of the playback shall also represent historical data with corresponding time-stamp.

The user shall be able to view the stored data on SCADA/EMS system displays such as on Single Line diagram, Network Diagram & Trend display by placing a workstation console monitor in a history mode for a specified time and date. Any system displays subsequently called up on that monitor shall display the data that existed at the specified time and date, or the closest previous time available.

The history mode and the historical time and date shall be prominently indicated on each display. The display during playback should confirm with all the facility of Network Status Processor as applicable in real time displays i.e., de-energized portion of the network, connectivity, Alarm-based visual effects (e.g. Thickening and blinking of lines, etc.) shall be shown accordingly.

The users shall be able to select the time window of interest to save part of above data in a separate file (file name of the playback data file could be user editable for describing incident/disturbance data contained in the file) for archival of above important data in the Historian system for future retrieval and playback in SCADA system. This archived data shall be transferable in database of Historian system for generation of reports. The snapshot of archived data shall be used by EMS applications in study mode.

The users shall be able to retrieve and playback data on geo-spatial maps, Single Line Diagrams, Other Displays and Dashboards defined by users. The playback feature shall have functionality of multiple re-constructions by different users working simultaneously.

Trending of any Analog Data should be possible during playback period. Playback can be done in same display no changes shall be required for HDR, only selection required input shall be required.

1.3.6 Alternate/Redundant Data Source Processing

All data in the SCADA/EMS database shall be obtained from more than one source and there shall minimum five (5) number of alternate sources for a point. Typically, the "best available" source of the data shall be chosen for use in displays, reports, and other functions. This feature of choosing the best available source is "redundant data source processing" function. The inputs to alternate/redundant data processing function shall be called "arguments", and the chosen source is called the "resultant best value." The arguments may be real time telemetered values or ICCP telemetered values or the values from the backup Control centre (if available) or calculated values, Application output etc. SCADA system shall support processing of same data from minimum 5 (5) number of alternate sources for a point.

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 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.

Users shall be able to override automatic selection and manually select any argument. Restoration of automatic alternate data processing shall require manual action by a user. Automatic and manual changes of the selected argument shall be reported as an event.

Alternate Data Source Processing methodology should be as follows-

Priority-1: Data reporting to SCADA from ICCP/FEP along with multisite data shifting between Main & Backup Control Centre (depending on data quality) will be primary source for data. System should automatically take the Backup Control centre without any configuration.

In addition to the above user should be able to configure additional sources of data for the same SCADA data field/point as-

Priority-2: Redundant data field/point.

Priority-3: Calculation data field/point.

Priority-4&5: Other application (internal/external) data field/point.

Functionality of defining alternate data points shall be available on same SCADA point and no separate SCADA points shall be configured.

With the above functionality we should have user selectable Negate and Block feature to the alternate sources of data.

1.4 Network Status Processor

The SCADA/EMS systems shall be provided with a power system network status processing function which shall be integral part of SCADA system and SCADA database. The function shall run automatically without any manual intervention.

All elements modelled in SCADA database should be considered while running Network Status Processor.

This function shall be capable of analyzing the open/closed status of switching devices, such as Circuit breakers and Isolators, in order to define the configuration of the substation for display. The energization of all power system elements such as lines, transformers, bus-bars, generating units etc. shall be determined so that the associated displays may correctly show the status of these power system elements. The energization, de-energization (line open from both ends) and partially energized (line open from one end) of all power system elements shall be distinguished. The configuration shall be re-evaluated and updated whenever a switching device status change is detected by the system.

The connectivity for Network Status Processor shall be defined while configuring SCADA database only and it shall be processed automatically without any user intervention or external scripts.

All element modeled in SCADA database should be considered while running Network Status Processor.

Network Status Processor shall be able to compute availability of elements in real-time and given duration of interest based on historical data of output of NTP.

1.5 Sequence-of-Events (SoE) Recording

SoE data is the time stamped chronological/reverse chronological listing of status change/events collected from the RTUs directly and through connected control Centers on ICCP. The SOE data is time tagged with one millisecond resolution and there shall not be any discrepancy in the SOE timing in millisecond resolution, from any RTU to the control centers.

SoE data shall be collected by the system and shall be made available for review by user. All necessary processing required on the SoE data like filtering, sorting, merging, mapping (voltage, element type, area, region, station etc) is to be done at the control centre. It should be SOE data acquisition shall not interfere with periodic data acquisition from other control centres.

The description of each event shall include the device name (Alias Name), in addition to database description name, device state, the date, and the time (to the nearest millisecond) of each event. Events shall be displayed and logged in chronological order. The user shall be able to select the display of events by element type, voltage level, region, area and stations, or the entire power system covered by the control centre.

All SoE data shall also be stored in Historian system throughout the contract period. There should be provision to see SOE monthly/weekly/daily/hourly/any user defined time period, on demand for last six-month period within 1 minute and based on various filters like voltage possible to take output in csv, excel format, pdf etc. and publish in the webserver through secure manner. User Interface must be same for seeing the current SOE or older SOE coming through either RTUs or over ICCP. Logs should be made regarding all the points not merged and entered into the database.

SoE should be visualized in a User Interface (as integral part of SCADA system) with filter and sorting. Generation of reports based on various filtering option (elements type, Voltage, Region and Station etc) shall be provided.

1.6 Supervisory Control

An appropriately authorized user of a control centre computer system shall be able to control the operation of field devices connected to RTUs. Control command can also be given from other control center through ICCP.

The devices that can be controlled from any console shall be determined by the controlled authority assigned to that console and user. It shall be possible to assign a number of controllable devices in one group and then control all the devices by executing a single control command on the group. The Control centre computer system shall in turn execute the supervisory control to the various devices in the group as required by the communication protocol sequences.

A control action shall require a confirmation-of-selection-prior-to-execution response. Initiation of the control execute step shall occur after the user confirms that the correctpoint and control action have been selected. After the user initiates control execution, the interlocks defined for that device shall be checked, the RTU shall be addressed, verification that the correct point has been selected at the RTU shall be obtained, and then the control action shall be executed.

If, after selecting a point, the user does not execute the control action within a programmer-adjustable time-out period, or if the user performs any console action other than completing the control action, the selection shall be cancelled and the user informed. The user shall not be prevented from requesting other displays, performinga different supervisory control action, or performing any other user interface operation while the master station waits for a report-back on previously executed control actions. The device undergoing control shall be highlighted by the Computer system with a different color/graphical attribute so that it is identifiable by the user. This highlighting shall be present till the receipt of desired feedback from the device.

The system shall process supervisory control commands with a higher priority than requests for data from the RTU data acquisition function.

1.6.1 Switching Devices

The user shall be able to select and operate any controllable switching device. Controllable switching devices will be of either the two-state or three-state type, e.g., circuit breakers or motor-operated disconnects.

1.6.2 Capacitor/ Reactor Banks

The user shall be able to control capacitor/reactor devices. The procedure for controlling these devices shall be the same as that of a switching device except that any supervisory control action must be inhibited for a programmer-adjustable time period after the capacitor/ reactor device has been operated. A message shall appear if an attempt is made to operate the device prior to expiration of the time interval.

1.6.3 Tap Changing Transformers

Depending on circumstances, the user may raise or lower the tap positions of On Load Tap Changing (OLTC) transformers. An OLTCs Supervisory/Local control mode, Master/Follower/Independent status, and tap position shall be monitored. Tap excursions beyond user-specified high and low limits shall cause the master station to generate an alarm. Supervisory control of OLTCs shall only be permitted when the transformer's control mode is Supervisory in conjunction with a status of Master or Independent.

All attempted invalid control actions shall be rejected. For supervisory operations, the initial selection and control of the transformer for a raise/lower operation shall follow the confirmation-of-selection-prior-to-execution procedure. Upon receipt of the raise/lower command, the field device will immediately execute the control action.

It shall not be necessary for the user to re-select the transformer for additional raise/lower operations; the user shall only have to repeat the desired number of raise/lower commands, which shall be executed immediately. Normal scanning functions shall not be suspended between the times that repeated raise/lower commands are issued. The user shall be able to cancel the operation or have it automatically cancelled by the master station after a programmer-adjustable time period elapses after the last raise/lower command.

1.6.4 Control Inhibit

The user shall be able to inhibit or enable supervisory control on any device. A tag symbol indicating the control inhibit conditions shall be displayed next to the device on all displays where the device is presented. The programmer shall be able to define the following 4 tag types with up to 6 tags per device:

a) Tag symbol and colour to be displayed (Red, Green, Yellow, White)
b) Tag priority
c) Type of controls that shall be inhibited by the tag (e.g., open only, close only,

open and close, or information only (no control inhibit).

Only the highest priority tag shall be displayed. Any combination of tags shall be supported, including multiple tags of the same type. The combined effect of multiple tags shall be to inhibit a type of control if it is inhibited by any of the tags. The user shall be able to place up to 6 nos. of tags.

When a tag is placed on a device, the system shall automatically assign a unique tag number and a comment of up to 60 characters. A list of all active tags on a device shall be conveniently accessible to the user. The list shall indicate the date and time the tag was placed on the device, tag type, tag number, and the user-entered comment for each active tag. Tag removal shall be permitted from this list and from any display where the Tagged device is shown. An event message shall be generated each timea control inhibit tag is placed or removed.

1.6.5 Control Action Monitor

The response to all control actions shall be verified by monitoring the appropriate feedback variable. A report-back timer (the duration dependent on the type of device) shall be initiated when the command is issued. At least ten timer periods shall be supported, any of which may be assigned to any device. System-wide timer periodsof 10 to 60 seconds and individual-device timer periods of 1 to 60 seconds shall be supported and shall be adjustable in steps of one second.

The user shall be provided with an indication that a control action is in progress and, subsequently, a report of the result. If the control was unsuccessful, an alarm shall be generated that states: (1) the control message exchange was not completed successfully, (2) the device failed to operator (3) the device operated but failed to achieve the desired result (e.g., following a close control action, a three-state device operates from the open state, but remains in the transition state). If the control was successful, an event message shall be generated noting that fact.

For commands issued as part of a group control or load shed operation, the successful completion of all device control actions shall be reported via a single message. If the operation is unsuccessful, the user shall be informed of those devicesin the group that failed to operate.

1.6.6 Power Flow Check-Before-Control

A "select power flow" option shall be available to the user prior to the requested supervisory control execution. When this option is selected by the user, a system-wide power flow shall be executed based on the latest state estimate and desired supervisory control action. The purpose is to advise the user of any potential problems due to the desired control action. The following features shall be included:-

(a) **Check-Before-Closing:** The following shall be displayed:-

- Initial voltage across open device
- Initial angle across open device
- Initial power system frequency difference across open device
- Load and generation pickup due to device closure
- Voltage violations due to device closure
- Overloads due to device closure.

(b) **Check-Before-Opening:** The following shall be displayed due to device opening:-

- Load and/or generation drop
- Voltage violations
- Overloads
- Electrical islanding
- Bus splitting
- Power system frequency

1.6.7 Interlocks for Supervisory Control

The Supervisory control action on a device shall be processed only if it is permitted by the interlocks defined for the device. The interlocks shall be defined while building the database model. It shall be possible to define interlocks by using any of the status and analog points in the Control Centre computer system.

1.7 Load Shed Support (LSS)/ ADMS

LSS/ADMS shall be used by the dispatcher to handle demand management efficiently and in a systematic way by shedding the load. It shall be implemented based on state requirements & regulations. The LSS/ADMS shall operate on load feeders in which provision of remote tripping through SCADA already exists or shall be made in future by Owner. Any work at substation end required for achieving tripping in field shall be in the scope of Owner. The scope of work at Control center end for implementing LSS/ADMS (for existing and future feeders) shall be in the scope of contractor.

Key features of load shedding functions are as:

- Load shedding shall enable an operator to shed or restore a list of load control element.

- Load shedding shall enable shed or restore to a specified MW load curtailment automatically using predefined logic.
- Load shedding shall enable shed or restore a percentage of the total available load in a list.
- Load shedding shall enable shed rotate shedding through a list of load control elements.
- Load shedding shall have LSS displays. LSS display shall have individual load MW amounts and relevant associated switch information e.g., status. LSS display shall consist detail of individual metered load values from telemetry associated with the load control element. LSS display shall have information pertaining to total Load shed, which shall be calculated as sum of the available loads within user-defined list, which have been successfully opened. LSS display shall have detail of the load shed lists and the current state of equipment.
- Load shedding shall have the ability to allocate portions (by percent/ratio/other means) of the total load shed requirement to the Load Shed Area/Group/DISCOM by manual data entry and to then initiate automatic calculation of corresponding load shed suggestions to the dispatcher.
- It shall be possible to define Linear and Circular type load shed groups.
- A Linear-type Load Shed Group shall be defined as a group of loads in which load shed begins at the load element designated as start point and proceed to the end of element list.
- It shall be possible to define logic for automatic Load Shedding or restoration using various combinations of system parameter as per Owner requirements during entire life cycle of the project.
- A Circular-type Load shed group shall be defined as a group of loads in which load shed begins at the load element marked as start point. In Circular type load shed group start point is shifted to the next to the element(s) who participated in load shed after each load shed. When the end of the list is reached on subsequent shed operations, the start points designation wraps (i.e., circles) back to the first element.
- It shall be possible to assign a load to a Linear or Circular type load shed groups.
- LSS shall have feature of trigger-based load shedding based over critical system parameters (i.e., frequency, over-drawls, under-drawls, under voltage etc.). If the values of these parameters are crossing the thresholds, LSS shall start shedding of pre-configured loads. The load feeders/load

groups are tripped in the order of time-based priority as defined by the operator. The loads with the lowest priority are disconnected first

- In addition to the amounts of load to be shed, LSS shall include provisions for displaying the current load shed capacity.
- Load shed capacities will indicate how much potential load shedding is available.
- Provision to save reports in different format like PDF, EXCEL etc. as per requirement of Owner. There should be provision to print the reports as per requirement.
- There should be provision to send email/SMS for the information of the trip signal generated to designated user.
- LSS shall maintain a daily history of the load shedding (feeder/bus wise and Summary) performed. This information shall be available for display and modification via manual data entry.
- LSS shall have feature to implement load restoration.
- LSS shall also provide a means of allocating portions of the State's total load restoration requirement to Load Shed Area/Group/DISCOM by manual data entry, and to then initiate the automatic transmission of corresponding load restoration.
- LSS shall update the status of the load restoration process based on the manual entry by dispatcher/Telemetry information collation of the amounts of load actually restored. Subsequently, the dispatcher shall be able to prepare and send further load restoration.
- LSS shall have feature of pausing shedding/restoration process. Once paused, the operator may resume, or abort the process.
- LSS shall have feature of delays between shedding and restoring the load. It shall have feature of configurable delay before the restoration of load control elements to prevent immediate restoration of all selected loads. Two-time delays shall be defined for each load, one to be used during the shed process, and one to be used during the restoration process.
- LSS shall have feature to shed loads in assigned time-based priority. When a list is shed, the loads shall be shed in time-based priority order. Similarly, the loads shall be restored in the order they were shed.
- The LSS shall also monitor and collate information from SCADA on actual operation/performance of Under Frequency Relay (UFR) Load shedding. Under frequency relays monitor power frequency and respond to a decrease in frequency by shedding loads; the more the system frequency

drops the more load is shed. The under-frequency relay monitoring function shall monitor and report the status of the under-frequency relays, monitor and report the status of the associated feeder breakers, log all under frequency events pertaining to both the relays and the feeder breaker switches, and calculate the amount of load shed and available load to shed Application shall record the MW values from selecting measurement points before and after the change in the state of a selected under frequency relay. The MW flow associated with each under-frequency relay shall be stored in the database. This stores value shall be summed with other flow values to produce a total under-frequency shed.

- LSS/ADMS data such as tripping data, logs etc. to be stored in historian system provided under the project.

1.8 Historian

The purpose of Historian is to facilitate storage, archival and retrieval of process parameters for creating information through comparison and contrast and messaging of stored values to create valuable information for business of grid operation.

Historian system shall store all real-time SCADA fields and their quality codes, all Estimated process values, all Calculated values, SoE, complete data of EMS, complete data of AGC, DSA outputs, logs, NMS output, reports, weather sensor data etc. in an auxiliary memory, and also provide the means to access this data and display it through high-quality graphics, plots, trend and Management Information System (MIS) reports.

Provision of configuring any database field/point for archrival shall be there in historian. The historian shall also store data as mentioned in different clauses of the specification in secure manner.

Functionalities mentioned under this section (including visualization) shall be met by the Historian itself and from SCADA wherever specifically mentioned. The proposed solution shall be COTS product and as per COTS definition specified under the technical specification and BoQ. Historian shall be able to provide dedicated dashboard and different types of graphs as PART-B, Appendix-N apart mentioned herein under.

1.8.1 General Requirements

The Historian System shall capture raw production data in real-time, at its original scan rate from the SCADA system and also from other specified sources such as database fields/points of ICCP, EMS, AGC and DSA etc. This includes storing of data such as SOE, Analog values, Status Values, calculated values, Energy Values, external inserted values etc. The raw data can be captured either by exception or periodically.

The Historian System shall be a COTS (Commercial off the Shelf) product and shall provide user-configurable graphical visualization, reporting, analysis, and web application/access tools. It shall display current and past operating conditions on desktops anywhere and anytime throughout the enterprise and beyond. It shall store the information online for at least **seven (07) years** at its original resolution, making it instantly available for deep and broad analysis, trending, and benchmarking for continuous process improvement.

The Historian System shall provide operators, engineers, and management with direct access to one integrated source of information. The Historian System shall also provide the ability for any users to view SCADA data beyond control center across the organization. The Historian system shall support standard query-based information retrieval as well as interaction through pull down menus.

Historian system shall provide provision of insertion of future values in Historian. A user-friendly API shall be provide to transfer the values from Historical server to SCADA server. The user can add/delete/edit any no. of points to be transferred. All type of data including analogs, digital status, etc. shall be automatically configured in Historian without any manual effort as soon as reflected in real-time SCADA database. There shall be provision to extract filtered data from the historical data on the basis of user's requirement. The facility to fetch data from historian shall be user configurable.

The facility of bulk editor shall be provided for example fetching data of specific voltage level, filtering out all isolators in the state etc. Further, the feature of filtering data based on parameter wise (e.g circuit breaker of any voltage level, isolators of any voltage level etc.) , device wise (e.g transformer, lines, capacitors etc.), substation wise (e.g. list of substation having interstate lines etc.) shall be provided. The Historian System shall provide the feature of sorting of data based on type of substations (generator, transmission, cogen etc.), zone wise etc.

1.8.2 Configuration of the Historian System at Main and Backup Control Centres

The Historian system shall be supplied at main and backup control centers. The Historian System shall communicate to the SCADA servers and sample the real-time values as configured by the User. The real-time values shall be stored at the same resolution as available from the SCADA server.

Historian at main control centre will receive data from SCADA at main control centre as primary source and data from backup control centre can be synced as per user selectable date and time range on requirement. Similarly, Historian at back up control centre will receive data from SCADA at back up control centre as primary source and data from main control centre can be synced as per user selectable date and time range on requirement.

Typical architecture of historian data reporting to Main and Backup control center is given in **Part-A Appendix-F**.

Similarly, Historian at back up control centre will receive data from SCADA at back up control centre as primary source and data from main control source as secondary source. Control centers will be configured to have no effect on a single point failure, which means even if one of the historian servers is unavailable, the other shall automatically take over the functionality.

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 collection and processing to the revised database.

The Historian system shall have feature of the manual correction of the archived data with a unique flag. This shall be limited to only to the authorized users. All such changes shall be logged to the audit file for future reference. The Historian system shall have feature of creation of forms and screens for manual data entry. An API to be provided for bulk insertion of manual data on schedule basis/or on demand. Also, for insertion of data, through manual uploading of files shall be provided.

The Historian System should support high availability and automatic failover, interface data buffering of at least 72 hours to guarantee no data loss, and no impact to clients or applications in case of communication loss or data server shut down for maintenance or security patch installations, etc.

Software utilities shall be provided in the Historian System to back-up the Historian data **in a redundant SAN and backup appliance** available on network. This software shall have the feature of automatic as well as the manual backup of data. This utility shall also provide the feature of retrieval of data for selected period to be used in generation of reports through user-friendly pull-down menu and drag and drop facilities. The typical types of data and its periodicity to be stored in Historian system is enclosed at **Appendix-I.** The same shall be finalized during the detailed engineering Stage. The tentative sizing of the Historian is mentioned in **Appendix-F**.

The Analogs, Digital Status, etc. shall be automatically configured in Historian without any manual effort as soon as it is reflected in SCADA database after database on-lining.

1.8.3 Features required with the Historian System

The following features shall be provided along with the Historian System application:-

a) Interface with SCADA software for acquiring the real-time data

The Historian System shall exchange data with the SCADA system and ensure high performance for real-time data exchange. The data value as well as quality codes shall be received from the SCADA system. Data must be time stamped according to the sending system and not on receipt by the Historian System unless no other time stampis available. The Historian System must store all the time series data in its original time-resolution and associated quality code in a real-time database. Historian should have an interface to send the output of calculations periodically/on demand/event based to SCADA.

b) Organization of data and configuration

The asset or power system topology model hierarchical structure shall be stored in Historian System with versioning/archiving capability, and with roll-ups to aggregate data on real-time basis. The Historian System must be able to link data points held within the Historian to the process model defined in SCADA System.

c) Real-time data interfaces

The Historian System shall provide real-time, fault-tolerant, high-speed links from any industrial automated real-time data sources through an industry standard interfaces such as multiple OPC industry standards, OPC DA, OPC UA and OPC HDA, connector. Also, it shall have interfaces compatible with DAS (1.0a and 2.0) compliant servers, **SOAP, REST,** SQL, ODBC, OLEDB, Modbus, ASCII, and text. The data historian shall provide the trace logs for audit trails and audit purpose. The Historian system shall have interface to integrate with any Business tool (for ex: Tableau, Sisense) for supporting functions like reporting, graphical visualization, analysis etc. User shall be able to configure dashboard based on historian data and shall also be possible to select various types of graphs in single dashboard. The Historian System shall provide the trace logs for audit trails and audit purpose.

d) Calculated values

The Historian System must be able to perform any mathematical calculations on raw data values (analog and digital values) before being displayed. The user interface shall be provided to perform all type of calculations. The Historian System shall also have data summary function for defining calculations such as totals, averages, and other aggregates from real-time data **and historical data input points available in historian on the fly. Summarized functions/calculation created can evaluate the output on the existing historical data points also**. The equations of these calculations shall be able to use mathematical functions, logical operators, conditional operators and trigonometrically functions. Calculations shall be started and reset based on time.

The Historian System must be able to save calculated values as separate data **fields**/points **within historian directly (independent with SCADA database)**. The Historian system shall perform the calculations in real time and allow results to be trended and archived with the raw data without affecting the operations of the source systems. A proper web-based GUI shall be provided to perform various type of calculations.

The historian shall provide functions such as derivative and double derivative to compute the" ramp rate" and "rate of change of ramp rate. Historian system shall provide moving average on a user configurable time interval as per requirement.

The calculation engine shall be able to define calculation functions as aggregations; based on equipment type, system voltage, station-wise, region-wise, area-wise, asset type, totalizers (accumulators), and performance equations formulas and shall support periodic or time-based or event-based triggers. The calculation expression shall allow the users to implement complex calculations without any formal programming and coding. The calculations shall be able to be done by asset-based/group-based, insteadof per-point basis. All calculations shall provide the re-calculation functionality to automatically or on-demand to re-calculate the historical data. The calculation tool shall also have:-

a. Ability to define static variables.

b. Ability to define logic-based expressions.

c. Standard math library.

d. Configurable calculation frequency.

e. Adding new calculation without affecting the existing calculation service.

f. Ability to define calculations with return error codes.

e) Graphical user interface

The graphical user interface shall be provided meeting all the defined functionalities. The User interface shall facilitate contextual organization of information for decisions making. The GUI shall create and display real-time and historical data, including customizable equipment schematics and trends, for faster evaluation by all the users. All defined functionality shall be meet through GUI (MS Excel shall not be used strictly); except export of defined reports.

The UI of historian system shall have following features:

- Drawing tools
- Ability to incorporate trends
- Easy to zoom-in/zoom-out capability.
- Drilldown
- To solve production issues quickly. Ability to produce ad-hoc and formal reports

on data held within the Historian and any linked databases.

• Reports shall be configurable for different time/region/substation ranges by simply changing the report time/region/substation cells.

• Ability for report to carry some manual entry.

• Excel based add-in Reports.

• The UI should have interface with MS tool and XML

• To generate dynamic repots in tabular format. Scheduling options to generate reports time-of-day scheduling, natural scheduling (when an input tags changes), event-based scheduling. End-users tool to build, modify and manage displays SLD (Single-Line-Diagrams) and multiple build-in analytics from amongst graphs, bar-charts (horizontal or vertical), XY plots (can be rotated in any direction), pie-charts, scatter plot, box-plot (refer to Appendix-B), heat map, GG Plots, Correlation Matrix ,violin plot, Density Plot, candlestick chart, histograms, 3-D plots, multi-state symbols, layers, etc. It shall be possible to extract the graphs on dashboard in .jpeg, .png, .pdf formats.

• Major and minor axis of plots shall be user configurable.

• Trending Displays configurable refresh rate.

• Comparison between different values stored in historian on same graph.

• Viewing rights for SLDs and other data analytics rights.

• User configurable dashboard/user interface/tool to create self-defined dashboard for historical data.

• The UI of Historian system shall have the capability for the data points to be presented in various formats. These shall include trends i.e., time series data, Tabular & Graphic and Static reports.

It shall allow users to create interactive, configurable displays/dashboard for publishing on the operator workstations as well as on the web. It shall be possible to extract the data for a user configured parameters and selected time period. User interface for drag and drop functionality shall also available. It shall be possible to search for a data point by defining search criterion in the system.

The Historian system shall provide a development tool to develop customized display screens. This tool shall provide the ability for developing their own display screen independent of user and workstation. It shall be possible to search for a data point by defining a search criterion in the system.

f) Interface with office applications

The Historian System shall allow retrieval of data into Microsoft Excel. It shall provide menus to extract data into spreadsheet. Extraction shall include current value, archive value, aggregation calculation (average, min, max, total, standard deviation) for specified period, tag-based calculation and calculations with filters.

g) Manual data entry

The Historian System shall have the capability to accept manual data also. This information shall be used to complete the picture of operations and required for problem diagnosis or reporting in conjunction with the data collected automatically. Manual data entry shall be allowed from defined clients with audit trail. An API tool to be provided for bulk insertion of manual data on schedule basis/or on demand.

It should also have feature manual uploading of files for insertion of data.

The Historian system shall have feature of the manual correction of the archived data with a unique flag. This shall be limited to only to the authorized users. All such changes shall be logged to the audit file for future reference. Bulk upload of future value shall also be possible which will be used to plot graphs.

h) Interface with Business Applications

A well-documented API shall be provided to exchange data in secure manner with third party software. The API must be able to query data and models held within the Historian System. The Historian System must offer connectivity to third party systems using multiple protocols(at least two) e.g; OPC/ ODBC/ OLEDB/ JDBC and web services. The Historian System must be able to control the authorization of data extracted through API.

i) Data migration requirement

The Historian System shall provide means of migration of data by importing and exporting old data in a predefined format such as .csv files or through APIs so that the data can be migrated to another system. It shall be the responsibility of contractor to migrate data from old system to new system. Old data for duration of 10 (Ten) Years needs to be migrated to new system. Sizing of the Historian System shall also consider this requirement. Creation of format, extraction and import of data from old to new system shall be the contractor responsibility

j) Interface with External System

The Historian system shall provide web services on SOAP and REST to publish data into the database through multiple applications.

Historian System shall have inbuilt OPC-UA Server functionality so that OPC Client shall be able to take the data from Historian system using a defined OPC interface. Historian system shall also accept data from OPC clients. OPC client licensing up to 15 clients shall be provided which is to be used in historian server as well as external system which will be used to import & export the data via OPC.

The Historian system shall also have an ODBC (Open Database Connectivity) interface which shall allow all the historical data to be accessible by Personal Computers (PCs) running Microsoft-Windows based applications. A dynamic link between the Historian system and the spreadsheet shall enable an automatic update of the spreadsheet whenever data point change.

k) Mass storage of files and Data

The Historian system shall also be used for mass storage of data and files such as EMS application save-cases, Output results of EMS applications, Outage Schedules and Continuous real-time data of selected time window. External file (i.e., monthly compiled data) shall also be stored for archiving and retrieving purposes. Requirement mentioned in this section for storing various files / save cases in historian system to be fulfilled by using SAN with proper back-up of it.

l) Sequence of event (SOE) data interface

Historian system shall store the sequence of event (SOE) data and shall generate report as and when required based on various filtering options. It shall be possible to import ID as well as detailed name of the imported parameter (which will be used during reporting). Proper log generation system shall be in place in case data available for archiving and not stored in historian due to some reason. SOE transfer in historian shall be through both automatic and on demand basis by operator. All stored data shall be accessible from any time period regardless of changes made to the database after storage of that data. Report generation of SOE shall be possible with sorting facility of parameter.

m) Additional <u>Scope for ERLDC only</u>: -Transferring data from the SCADA Information storage & Retrieval system to the SAN (Storage Area Network) of IT network.

This section outlines the scope of work and specifications for the Contractor responsible for securely transferring data from the SCADA (Supervisory Control and Data Acquisition) Information storage & Retrieval system to the SAN (Storage Area Network) of IT network. The objective is to ensure the safe and reliable transfer of sensitive SCADA data to the IT system while maintaining data integrity, confidentiality, and availability. This requirement shall be envisaged for ERLDC only with following objectives: -

- Securely transfer SCADA data to the IT SAN system.
- Maintain the integrity and confidentiality of the data during the transfer process and minimize the security risks such as unauthorized access, data loss, or tampering.
- Ensure the availability of all SCADA data including new datapoints that may be integrated in future in SAN of IT system.

The Contractor shall be responsible for the following tasks:

a) Assess and design SAN infrastructure of IT including its sizing, architecture, protocols, and security requirements as per SCADA storage system.

b) Design a secure data transfer solution that meets specific requirements and aligns with industry best practices and relevant regulations.
c) Supply, install and configure SAN storage with SAN management server and integrate the system in IT system.
d) Supply, Install and configure necessary database software along with require tools in SAN infrastructure of IT. The supplied database must not be proprietary and preferably be NoSQL database.
e) Required licenses of database for storage and processing of data must be supplied.
f) Install and configure necessary software, tools, or protocols required for secure data transfer.
g) Establish secure communication channels between the SCADA storage system and the IT SAN.
h) Set up appropriate encryption mechanisms to protect data during transit.
i) Implement access controls, authentication mechanisms, and authorization policies to ensure only authorized personnel can initiate or access the data transfer process.
j) Configure logging and auditing mechanisms to track and monitor data transfer activities.
k) Conduct comprehensive testing of the data transfer mechanism to ensure its reliability, efficiency, and security.
l) Verify the successful transfer of data from the SCADA storage system to the IT SAN without any loss, corruption, or unauthorized access.
m) Perform penetration testing and vulnerability assessments to identify and address any potential security weaknesses.
n) ERLDC/User shall reverse the right to do necessary processing of data from directly from the SAN system and integrate other analytic systems as per user requirement.

1.8.4 Reports

A Business Tool shall be provided with user friendly configurable with drag and drop query builder, report builder and trend builder facility. Reports can be generated on user demand, on a preset timed interval, or be driven by specific events. The contractor shall be required to generate the Daily, Weekly, Monthly and Annual reports formats. The output of the report shall also be available in csv, XML & MS office tools etc. The user shall be able to schedule periodic generation of reports, direct report to display, print report, and archive report using report scheduling display. It shall be provided to analyze all the data on spreadsheets with features such as automate daily reports, create dynamic reports for any area of operations, summarize years of data with figures like maximum/minimum/Average/Rate of change /other mathematical functions, create the custom reports for regulatory authorities, etc. For example –User shall be able to create dynamic reports in the form of spreadsheets with designated cells containing the required data specified by the user for a fixed time or period of time. The data can be raw SCADA value or any mathematical calculation performed automatically on the archived data. The report scheduling display shall enable entry of the following parameters, with default values provided where appropriate:-

(a) Report name

(b) Time the system should produce the report.

The user shall be able to examine and modify the contents of reports for the current period and for previous report periods using displays. Any calculation associated with the revision of data in a report shall be performed automatically after data entry has been completed.

The reports shall also contain the followings:-

a) Operator entered fields of English and Hindi text, symbols, images, etc.

b) Trends and Charts (2D and 3D)

c) Generation of data directly from dashboard for selected period

The reports shall be programmable as per user requirement. The user shall be able to generate report based on their requirement for example report of cogen and solar availability report, percentage availability report of analog & digital points voltage wise & individual substations wise, daily/weekly/monthly tripping report etc. The report for manual update/substituted values for Daily/weekly/monthly along with audit log shall be provided.

The sample of reports and displays is enclosed at **Appendix-B**. The detailed reports shall be provided during the Engineering Stage.

1.8.5 Historical Trending

The Historical trending facility in user interface of historian should have feature/facility to:-

a) Specify trend header

b) Rescale and Re-label axis

c) Three (3) dimensional plots, single surface, double surface for selected duration, parameter for data to be displayed

d) Zoom in and Zoom out on data by rubber banding

e) Selection of points through drag and drop features

f) Specify trending period i.e. start date & time and end date & time for trend orstart date & time and total trend duration.

g) Display the time stamp and value of all the trends for any point on the trend whilehovering over it with the mouse.

h) Save the configuration (trend point, data sample rate/interval, trending period,etc.) for viewing at later stage.

i) Configure up to **16 points** in a single trend window/viewport.

j) Plot raw, average, interpolated, min and max over a user defined sampled time.

k) On any displayed trend, it shall be provided to display its Max., Min. value, time and point on the trend of the trended data along with Average value as its magnitude and horizontal line to be displayed on trend window.

l) Compare up to 4 different time periods on the same plot simultaneously.

m) Comparison (trend) of two different days for the same parameter.

n) Customize trend properties such as Foreground and Background color, scaling, line color, thickness, font size, font type, plot style, type of data marker.

o) Overlay alarm thresholds on the trend display.

p) Plot of forecasted/future, scheduled value and its comparison with real-time should be possible for any duration.

q) Dashboard of Historian system and value of entire dashboard changes should be based on single selection of time/duration

r) Shall be able to put two cursor points on the trend, with a feature to calculate the value difference between the cursor points.

1.8.6 Sizing of the Data Historian

As per the specification requirement.

-----End of Section1-----

SECTION 2

EMS SYSTEM FUNCTIONS

Table of Contents

Section 2 EMS System Functions

2.0 Introduction

This section describes the functions to be performed by the EMS Applications being procured.

2.1 Design Requirements

The Bidders are encouraged to offer their standard products that meet or exceed the specification requirements. However, the proposal will be judged by its conformance to the Specification. These products may be provided from its in-house baseline offerings, the computer manufacturer and established third-party software suppliers. The proposal shall clearly identify all deviations from the Specification to help Employer/Owner evaluate the degree of conformance of the Bidder's offering.

The System Design Parameters and Performance requirements for SCADA/EMS system are specified in **Part-B Appendices C & D**.

All the variable parameters of SCADA/EMS System, which require adjustment from time-to-time, shall be defined in the database and shall be adjustable by system users through graphic user interface displays. All periodicities and time intervals contained in the Specification that define these parameters shall be considered as initial values to be used for performance purposes. The adjustments made to parameters by the dispatcher or the programmer shall become effective without having to reassemble or recompile programs.

The specific requirements for output results are described along with the other requirements of each function. However, all results shall be stored in a form accessible for display and printing, whether or not explicitly specified in the particular subsection. Save cases are to be created and stored along with the real time sequence of Power System Analysis applications and accessible during the entire project life cycle. EMS applications results/output of any of the PSA application are to be periodically stored and exported in the standard formats like .csv, .xml files. Periodic export of the result is to be configured for external network. The application result storage details shall be submitted during detail design stage. The system shall be designed such that failure of single server or single peripheral device shall not render the system unavailable.

2.2 Power System Analysis

It shall have power-flow analysis capabilities for performing steady-state system analysis required in system planning and operating studies. Such studies include steady-state voltage variation, line/transformer thermal loading, active/reactive power supply problems, etc. It shall allow the user to easily manipulate the solution/system parameters, quickly and reliably to solve the power flow, and examine the results in comprehensive output tables or on graphics. It shall also provide the capability to import and export data in a variety of formats (including. raw (PSS/E) and standard IEEE format). The Power System Analysis (PSA) functions shall be used at Control

Centre computer system to:

a) Monitor power system operations

b) Analyze power system security problems

c) Determine corrective and preventive controls that may be used by operating personnel to minimize the impact of security problems on reliable and economic power system operation.

The PSA shall include the following functions:

a) Power System Model Update (PSMU) including Network Equivalencing

b) State Estimation (SE)

c) Bus Load Forecast (BLF) including unobservable buses

d) Transmission Loss Sensitivity Factors (TLSF)

e) Network Sensitivity Applications

- Line Outage Distribution Factors
- Generation Shift Distribution Factors
- Load Shift Distribution Factors

f) Contingency Analysis (CA) including ranking.

g) Optimal Power Flow (OPF)

h) Short Circuit Analysis (SCA)

i) Transmission Line/Corridor Capability Monitor (TCM)

j) Power Flow based on SE solution (Real time Power flow solution and State Estimation solution both should be available simultaneously with the associated element and their values to be exchanged with the SCADA measurements)

k) Area Load Forecast (based on Load Groups)

l) Breaker Flow Calculation (Based on node breaker model flow through each breaker (CB and Isolator both) is to be evaluated)

The principal PSA activities of Control Centre are summarized as follows:

a) Facility is to be provided to run PSA on Separate Network Model (National/ Regional/ State/Individual Control Area/ Voltage Level).

b) Facility to compare (bus voltage/angle/line flow/topology status wise) the latest solved power flow solution with previous solved solution.

c) Import and export a detailed CIM (latest Version) based model of the power system under its area of jurisdiction as well as Power System of boundary-regions (Nearby systems), consisting all the Network elements at 110 kV and above. The supplied system should support IEC 61970-452 (i.e., Equipment Profile), and IEC 61970-456 (i.e., Analog Measurements Profile, Discrete Measurements Profile, State Variable Profile and Topology Profile) standards.

d) Execute State Estimation using the power system model together with synchro phasor measurements and all telemetry obtained from site and other control centers. The missing telemetry data shall be replaced with suitable pseudo measurements. Option for executing State Estimator with or without synchro phasor measurements (magnitude & phase angle) shall be available with the operator i.e., State Estimator shall have capability to accept voltage phase angle also as input for some nodes in addition to voltage magnitude. Feature should be available for selection of PMU data Station wise and globally also. EMS application should have compatibility with C.37 protocol for exchange of synchro phasor measurements directly from the available PDC of the control center. List of measurements where PMU data is being used in State Estimator should be available.

e) Listing all Circuit Breaker and Isolator which can be filtered voltage level/ station/area-wise in case the telemetered value is more than the threshold limit. On click, the user shall be able to navigate to corresponding single line diagram of sub-station containing the Circuit Breaker/Isolator.

f) Listing all Circuit Breaker which can be filtered voltage level/station/area-wise showing status in SCADA and in PSA Applications. Sample Display attached in **Appendix B(B-23).**

g) Execute other real-time PSA functions (e.g., OPF) using the base case obtained from State Estimation.

h) Perform PSA studies, using the Control Centre model together with the Control Centre's relevant operating plan.

i) Facility should be provided to evaluate time elapsed to run each application.

2.2.1 Data Entry, Manipulation and Verification

All input data in application shall be entered and viewed using data tables. The Data tables shall be used to display data of all components in the system. The user shall customize these rows and columns of tables to show data for a defined subsystem and/or in a specific order. In addition, application shall have single-line diagram (SLD) and station diagram (SD) features, which allow the user to create such diagrams by using a few straightforward techniques. Two display modes shall be made available for the graphics: system/station view and bus/component (node breaker) view, to suit for different applications.

Data changes shall also be applied by rules, for example, scaling load, generation, and shunt. The data table shall have the capability to import data from other applications also including Excel, CSV etc. All power flow data as well as SLD/SD shall be exported to other applications in a variety of formats (such as Excel). The application shall offer a comprehensive set of data sanity check functions including the following –

- Network topology checks such as identification of isolated buses, islands and parallel branches (lines & transformers) with the same ID.
- Isolated components in a station, branches in a station, transformers and compensators between stations.
- System parameter checks such as branches with unusual parameters, transformers with unusual tap ratios, and negative load/generation.
- Other possible data problems such as branches connecting buses at different kV, duplicate bus names, buses controlled by more than one device, and non-identical parallel transformers.

2.2.2 Modelling

Application provides a full range of power flow models as well as advanced models such as:

- **Generators –** All conventional, Renewable energy and storage model shall be included**.** The model shall allow local or remote voltage control within reactive power limits.
- **Loads -** Voltage dependent & frequency dependent (eg. induction motor load) load shall be modelled by a combination of constant current, constant impedance, constant MVA, and functions of voltage with non-integer exponents.
- **Switchable Shunts -** The model shall allow local or remote voltage control by adjusting shunt admittance discretely, continuously or according to a droop characteristic (for SVC).
- **HVDC Links -** Two-terminal and multi-terminal HVDC systems with LCC and VSC shall be represented in application with comprehensive converter models and flexible DC network configurations.
- **FACTS Devices -** Popular FACTS devices, such as SVC, STATCOM, TCSC, TCTCT, TCPST, and UPFC, shall be modelled in application.
- **Node/breaker Models -** Detailed node/breaker models shall be represented and arranged by the power plants or substations in which they are physically located.
- **Other Models -** Pumped Hydro, Lift Irrigation, Phase shifter, three-winding transformers, sectional branches, area interchange controls, etc.

2.2.3 Power flow Solution Techniques

In application, the following power flow solution algorithms shall be made available:

- Fast Decoupled Newton-Raphson
- Full Newton-Raphson
- **Automatic -** The Fast-Decoupled method shall be used first and the solution method to be switched to Full Newton Raphson, if necessary, to achieve faster convergence.

During power flow solutions, various power flow controls shall be available for getting enabled, such as switchable shunt and ULTC adjustments, Var limits control, area interchange control, FACTS controls, etc. The application shall use an advanced technique for adjustment of devices controlling active and reactive power flows so as to improve the convergence of the power flow solution.

2.2.4 Power flow Solution Reporting

After a power flow solution, the user shall select from a wide array of output reports including:

- Mismatches of the solved power flow.
- Individual component summaries (voltages, flows, etc.)
- Subsystem summaries, such as load, generation, losses.

In addition, a number of solution checks shall also be performed:

- High/low bus voltages.
- Branch/transformer overloads.
- Failed or violated generator controls.

The Power flow solutions shall be shown on SLD and SD. Any criterion violations shall be indicated with custom colors.

2.2.5 PSA execution and Model requirements

2.2.5.1 Real-time Mode

SE shall execute upon the occurrence of any of the following triggers:

a) Periodic (selectable between 2 minutes and 60 minutes, initially 2 minutes)

b) User demand

c) Event resulting in power system topology change.

However, it should be possible to disable any of the above options

Necessary Features of Real-time mode are listed as follows:

a) Event triggers shall take highest priority, with demand triggers higher in priority than periodic triggers. SE shall ensure that the input data represents a quiescent state of the power system which can be defined as no status changes have occurred for a programmer-adjustable period (initially 5 seconds).

b) The other PSA functions shall execute following the successful completion of SE and individually on demand. A separate count shall be specified for each of these functions for each trigger type, and each function shall be executed after SE has executed the number of times that the count is used to indicate.

c) OPF shall be initiated whenever an actual security violation (e.g., voltage violation or branch overload) is detected by SE. It shall then continue to execute after each execution of SE as long as the security violation exists or the output of one or more generators is being constrained to correct or prevent a security violation.

d) A record of the time shall be kept when each PSA function previously executed successfully and when the input data for such was last changed. Total time elapsed (difference between start and end time of PSA function) for execution of each PSA function to be evaluated and shown with PSA records.

e) The limits used for all applications shall be taken from SCADA application by default for each PSA application. However, the user shall be able to define and change multiple sets of limits for multiple parameters separately for each PSA application-wise (TTC, CA may use different sets of limits) in a single activity.

2.2.5.2 Multi-user Study Mode

a) SE, CA, OPF, TCM, PSA shall be executable at the Control Centre in a multi-user study mode environment; there shall be provision for concurrent user studies at each work station. Study mode should be able to take the real-time SE snapshot periodically or as per user demand. While fetching snapshot the study scenarios setup by user should not get over-written by the SE snapshots.

b) It shall be provided to compare output (i.e., Branch flows (both MW & MVAR), Bus voltages & Angles/ topology status) of multiple study cases (minimum 20 scenarios) of SE, CA, OPF, TCM, NSA applications by a single user. User shall designate any one of the 20 scenarios as a reference scenario and select some or all cases from the balance 19 cases for comparison with this reference scenario using inbuilt functionality. The results shall summarize the differences in input and output data with respect to the reference case and be available for viewing and printing. It shall also be provided to show two (02) study results of an application on the network diagrams and SLDs concurrently in different viewports. User shall be able to define database fields for the comparison of the cases.

c) Input for SE in the study mode shall be historical SCADA data saved by Real-Time Database Snapshot or from the current real-time SE solution. It shall be provided to scale load and generation on the basis of control area-wise and also node-wise before running study.

d) User shall be able to evaluate/study network condition in future. User shall specify the time and based on the time system shall retrieve all the relevant schedules before running the PSA functions. It shall be provided to scale load and generation on the basis of control area-wise and also node-wise before running study.

e) Input for the other functions shall be from stored SE or power flow solutions.

f) All solution and tuning parameters shall be separately specifiable for the real-time and study modes.

g) Users shall be able to validate and scale input case data and examine & compare the output data from different solutions. Any user shall be able to suspend preparation of an input case and to prepare and execute a second case without losing any data previously entered for the first case.

h) All PSA functions shall be capable of solving networks with at least 10 electrical islands. The model parameters shall be in per unit (p.u.) on a 100 MVA base.

i) System shall have provision of saving SE solution (every run of SE) for a period of one month.

2.2.5.3 Alternating Current Model

The Common Information Model (CIM) is a standard way of representing power system resources as object classes and attributes along with their relationships. The CIM facilitates the integration of EMS developed independently by different vendors.

The EMS-CIM should be able to do conversion of third-party network model formats to CIM compliant model and vice versa. The bidder should provide the Interoperability test compliance report for a set of different vendor and transfer of static data of CIM model along with the technical bid.

It shall be provided to export data model in CIM format (Latest Version) and web-based XML schemes as well as import from same.

The CIM shall be used as the foundation to maintain, distribute and exchange the static data. This data exchange would include all models and model files.

The minimum requirements of the Alternating Current (AC) model shall be as per the CIM standard IEC 61970-301 (i.e., Energy Management System Application Program Interface (EMS-API): Common Information Model (CIM) base). The offered model shall include:

a) Shunt capacitors and shunt reactors

b) It shall represent variable series capacitor.

c) There shall be no restriction on the magnitude or sign of the active and reactive components of the branch impedances.

d) Branches and shunt elements shall be identified by names and by their connected bus names or associated line names.

e) In EMS modelling, there should not be any limit in no of nodes under any station bus.

f) Limits for non-telemetered quantities shall be user- enterable.

g) Nominal ratios and step sizes for off load tap transformers shall be user enterable.

h) OLTC (On Load Tap Changing) transformer voltage ranges and step sizes shall be specified for each transformer. OLTC transformer impedances shall be adjusted as a function of tap position.

i) Phase-shifter angle ranges (or Target Power Flow) and step sizes shall be enterable by the programmer. Phase-shifter impedance adjustments with step change shall be automatic.

j) Transformers shall have low voltage and high voltage tap settings, one side with tap changing and the other side without tap changing. Programmer-definable gradient shall be provided for each transformer tap changer wherein effect of each tap can be defined.

k) Generator reactive power limits shall be modelled as a function of the active power output of the generator. Programmer-definable and user-selectable multiple curves shall be provided for each generator (including synchronous condensers). A single user action shall enable/disable generator reactive power limiting on all user-identifiable units.

l) Loads shall be generally modelled as:

   I. Constant active and reactive powers (by default),

   II. Constant Current

   III. Constant impedance,

   IV. Mixed

m) When there are several transmission lines between two buses and/or when the line(s) between the buses consists of several segments, a common name shall be used for each line with a separate individual line and/or line segment identifier.

n) Open-ended branches shall be modelled and the solution shall include:

   I. The voltage magnitude and angle at the open end

   II. The voltage and angle difference between the open end and the bus to which the branch is normally connected.

o) Designated generating units shall be capable of operating as synchronous condensers and/or pumps.

p) Static Var Compensator (SVC) models that recognize both voltage and susceptance control modes shall be provided.

q) It shall be possible to model a continuous controlled variable reactor such as to represent variation from zero value to Rated value as a function of voltage control.

r) It shall model Flexible A.C. Transmission Systems (FACTS) devices such as Thyristor Controlled Series Compensator (TCSC), STATCOM, Thyristor Controlled Phase Angle Regulator (TCPAR), etc.

s) It shall model Renewable energy sources such as Wind generator, Solar generation and Battery Energy Storage System (BESS) including electrolyser model as per IEEE standard, WECC generic models & user defined model. Model type with attributes will be decided during the finalization of the engineering document.

2.2.5.4 High Voltage Direct Current Model

The High Voltage Direct Current (HVDC) model shall represent the both, the DC transmission system and Back to Back station under Power System Model. The HVDC transmission system consists of DC transmission lines and associated converter stations and back-to-back stations without any DC Transmission line.

Each converter is an operating unit consisting of an AC switch, a converter transformer with OLTC, the DC valve, and a by-pass switch. AC harmonic filters and capacitor banks are connected to the bus on the AC side of the converter, which provide reactive requirements of converter. In addition, the converter is connected to the DC line through reactors and DC filters to limit fault currents and to smooth high-frequency components of the DC current.

Reactive Power Controller (RPC) is provided in the DC transmission. The purpose of RPC is as follows:

a) Prevent over voltages

b) Keep AC voltage within limits

c) Control the reactive exchange with the AC system

d) Ensure that the maximum connectable shunts are not exceeded.

e) **Ensure that the minimum number of AC filters are connected.**

Typically, RPC has two operating modes:

I. Automatic: Filter/shunt capacitor switching is performed by RPC, without user action.

II. Manual: Filter/shunt capacitor switching is performed by user action.

Transfer of control between Automatic and Manual modes is a user action and needs to be configured in a similar manner. The RPC also has the following two control modes in Automatic mode:

a) Reactive Control: RPC regulates the reactive power exchange with the AC network within a user-adjustable band of a reference value set by the user. Control is subject to constraints imposed by AC voltage limits or maximum connectable shunts.

b) Voltage Control: RPC orders appropriate filter switching whenever the AC bus voltage is outside limits set by the user.

The control modes are user-selectable and can be changed according to the needs of the AC system.

The HVDC model should have the ability to include Multi-terminal HVDC and VSC

(Voltage Source Converter) along with conventional models of HVDC also.

2.2.5.5 HVDC Model Application

All PSA functions shall include an HVDC model appropriate to the function being performed. The model must include an accurate representation of the compensation needed to supply the reactive requirements of the DC conversion process. Although a detailed model of the DC equipment and configuration is not required, the model must include:

a) AC reactive compensation equipment connected to AC bus
b) Invertor and rectifier reactive power coefficients
c) Minimum and maximum MW
d) Minimum and maximum firing angle. Following configuration of LCC and VSC based HVDCs may be specifically mentioned from modelling perspective:

   LCC

- Monopolar (with ground and dedicated return)
- Bipolar (with or without metallic return)
- Multi-terminal HVDC

   VSC

- Symmetrical Monopole
- Bipolar (with or without metallic return)

e) Mode of operation: ground return or metallic return (to adjust DC resistance of line)
f) RPC status (Auto or Manual, Reactive or Voltage control)
g) Filter criteria for monopolar and bipolar modes
h) Required voltage or desired MVAr requirement for both bipolar and monopolar operation modes.
i) Provision for putting different MW limits based on the mode of operation
j) RVO mode operation.

SE shall use real-time measurements of the DC MW value and the status of the shunt capacitors and filters.

The mode of converter operation (inverter or rectifier) shall be determined by the direction of active power flow. The DC terminal operates as an inverter when power flows from DC to AC and operates as a rectifier when power flows from AC to DC.

The reactive demand of a converter (QDC) is typically a quadratic function of the DC MW power flow as follows:

QDC = A*MW*MW + B*MW + C

The coefficients A, B and C are signed constants that are database-definable for each rectifier and inverter mode. Separate sets of coefficients shall be maintained for bipolar and monopolar operation. QDC is based on the total entered MW value. When operating in the bipolar power control mode, each converter's requirement is one-half QDC.

The DC line flow shall be included as interchange where appropriate. PSA shall monitor the AC regulated voltage and reactive injection based on input criteria, determine when reactive compensation needs to be switched and perform the required switching operation.

Contingency Analysis shall treat the DC line in the same fashion as other elements. In addition, it shall be possible to select one or more DC poles (with provision to club DC bi pole under single contingency) and the associated terminal equipment for inclusion as outage of element and HVDC setpoint reduction in a single contingency case. Sudden change in the HVDC flow should also be configurable as HVDC contingency in Contingency Analysis application.

2.2.6 Power System Model Update

The power system model to be used by SE and other power flow calculations shall reflect present conditions as reported by Telemetry, ICCP data Exchange from connected Control Centers and as entered by the users. The Power System Model Update (PSMU) function shall include the features mentioned in sub-sections below.

2.2.6.1 Network Topology

The prevailing network topology shall be determined from the status of all switching devices that affect the topology of the network modelled, e.g., a utility's internal power system network. This topology and the associated model parameters shall be based on:

a) Telemetered switching device statuses,

b) Manually entered switching device statuses,

c) Manually entered in-service or out-of-service designations for bus-oriented model elements (e.g., branches) where switches are not represented,

d) Modelled element statuses from the Outage Scheduler.

A separate display shall be available where there is mismatch in the status of a switching device and MW and MVAR flows on a device are more than threshold limit specified by user on per unit basis. **A specific display to show the list of switching devices which should be CLOSED shall be made available to the user Bus Loads**

Bus loads shall be calculated for the unobservable regions of the power system model by the Bus Load Forecast function described below.

2.2.6.2 Control Centre Power System Model

The Contractor shall develop Control Centre power system model as provided by the owner in the form of CIM model, Paper Copies of Single Line Diagrams, MS-Excel Sheets, etc. as per the availability with the owner. The Control Centre Model shall include the entire network **(generally 110kV and above, HVDC, etc.)** for the Control Centre operating area as agreed during engineering.

2.2.7 Network Reduction Methodology

For large interconnected Power System, the entire modelling of a large power system is not required for various power system study application. Hence, when the behavior of a part of a system is of interest, then the distant portion of a large interconnected network do not require a detailed modelling. For a given power system, PSA application is required to have complete network model along with reduced network model. User shall be provided software for network reduction using both the methodology:

a) Network Truncation.

b) External Equivalent.

The supplier shall provide software, which will be able to reduce the network based on selected boundary busses. The user shall have flexibility to define the network for making reduced network model based on the chosen nodes, bus, voltage levels, operating areas, regions etc. using Network Reduction by External Equivalence. However, Network Truncation may be used in selected network after consultation with the user

User shall be able to use the SCADA/EMS System to develop and export & import the equivalents in standard format of PSS/E and IEEE. The export format in PSS/E and/or IEEE shall be in latest version with backward compatibility.

The solution (voltage, Angle & Power flow) of equivalent or truncated system shall not have major variation with the full network's solution.

In real-time operator should be given options to select "Full network" or "truncated network" or "external equivalent network" for running of EMS applications as per real time sequence. User should be able to restore the original/full network model.

<u>Network Truncation:</u>

Supplier shall provide software which will be able to truncate the external network based on user selected boundary buses.

Network reduction tools should support followings while doing truncation: -

a) User can select boundary busses for truncation of network.

b) Equivalent load and generator shall be connected in boundary bus MW/MVAr telemetry of equivalent load /generator will be linked to corresponding branch or transformer. Equivalent load at the point of truncation should be frequency dependent (refered in section 2.2.2 bullet 2); because the same base case is to be used for DSA applications also.

c) An example of truncation is given below –While truncating the network at 400kV and above level, all the switching devices at 220kV and below level are opened in Network database and Modelled Loads are connected at the secondary side of 400/220kV ICTs. These modelled loads shall take the Real-time data on associated ICTs as its load measurements. A sample illustration for same is shown in **Appendix M (1-A).**

d) In case of non-availability of real-time data Bus Load Forecast shall be used for unobservable buses.

External Equivalence:

Network reduction software should support network reduction with external equivalent model. As base case is the pre-requisite for network equivalence hence, equivalent network could be used for DSA and DTS applications. The objective is to eliminate the external buses with some modifications at the boundary buses. The tools will reduce the network based on user selected internal/external buses. Boundary buses will be the buses of internal system which are adjacently connected with external system (system with set buses to be made equivalent for network reduction) with branch or transformer. Software will create equivalent branches with equivalent impedance amongst boundary buses.

Network reduction tools should support followings while making External Equivalence:

a) Allow the user to retain boundary buses or controlled buses as per his requirement. Facility to retain specific branches, generation, load based on user defined threshold in equivalent network. No manual intervention is required to reduce the network with external equivalent.

b) The software shall create reduced network for DSA as well as DTS application.

c) In case of incremental change in internal network, software should change in internal network and with no change in external equivalent. Software shall provide list of modified or new elements which are required to be added or modified. This is required to introduce minimum changes in existing tuned database.

d) In case of incremental change in external network, the software shall provide modified external equivalent network keeping the internal network unchanged. In this case tuned EMS database will not get affected and operator do not require any additional effort to tune the network. A sample illustration for same is shown in **Appendix M (1-B)**

Selection of boundary buses for Network Reduction is given in **Appendix M (1-C).**

After truncation of the network at a particular voltage level or region, it should allow for including a part of the lower voltage network as desired by the user.

2.2.8 State Estimation

State Estimation shall provide a complete and reliable power system model solution containing information for use by other PSA functions and for display. The State Estimator measurements will consist of telemetered data from sites and other control centers connected on ICCP links.

Performance statistics for SE to be available for Daily /Monthly/Yearly basis and shall be available in SCADA and Historian application

It may be necessary to convert certain measurements by other control centers for making it suitable for input to the State Estimator function. The Contractor shall provide functionality for merging/conversion of measurements received.

The State Estimator measurements will consist of telemetered data from modelled stations and real-time synchronized phasor data (magnitude & phase angle) from the URTDSM/WAMS system. In case where Telemetered data is not available pseudo measurements shall be used.

User shall be able to select algorithm for State Estimation (SE) out of Orthogonal and Weighted Least Square Algorithm.

2.2.8.1 SE Measurement Set

The measurement set for State Estimation will not always include sufficient measurements to estimate the state of the entire model. Therefore, the model estimated must be dynamically reduced to the limit of observability due to lack of measurements, loss of measurements and detection of anomalies. The portion of the model that is unobservable shall be solved either in conjunction with the observable portion or by a subsequent execution of the State Estimation algorithm based on the complete model.

The solution of the unobservable portions of the network shall be based on pseudo measurements for load profiles and generation profiles which shall be calculated internally from the system.

The preferred method(s) for calculating these Pseudo measurements are the following –

a) The unobservable portions of the model shall be divided into areas, each of which represents a Region or the unobservable portion of a Region.

b) For each Region the load profiles, generation profiles, and net interchange profiles shall be calculated internally from the system. Provision shall be made for these values to be telemetered. Alternatively, the State load shall be calculated based on the total Regional load and a predefined State load ratio, the net interchange shall be enterable by the user and the generation shall be calculated from the load and net interchange. This requirement shall be met either through SE or Optimal Power Flow.

c) Pseudo measurements for the load at each bus shall be calculated based on the state/regional load and pre-stored bus load distribution factors. Provision shall be included to use several sets of busload distribution factors based on time-of-day, day type, and month.

d) Pseudo measurement for the generation at each bus shall be calculated based on the status of each generator base point, in the event that the generator status if different from the Current Operating Plan. Otherwise, the generator status shall be as per the Current Operating Plan.

e) Pseudo measurements for unobservable regulated bus voltages shall be based on either a function of the load of the Region where the bus is located, or a function of time of day. Provision shall be made for a linear function of up to three segments of voltage versus load at each regulated bus.

f) When unmetered tap loads exist on transmission lines where the flows are known at both ends, pseudo measurements shall be based on the net flow into the line and bus load distribution factors. The bus load distribution factors shall be those maintained by BLF, normalized for all unmetered tap loads on the line.

g) When needed, pseudo measurements for regulated bus voltages shall be calculated as the mid-point between the high and low bus voltage limits from Limit Monitoring.

h) It shall be provided to substitute telemetry data for any pseudo measurement if telemetry is available.

i) Accuracy classes to be defined based on the type of measurements (Unit, Branch, Load measurements etc.). Based on the accuracy, weightage can be given on various data for SE.

2.2.8.2 State Estimation Characteristics

The State Estimation function shall:

a) Solve all islands when islanding occurs in the solutions due to either real electrical separation in the network or observability islanding. The solutions from the islands shall be integrated into a single network solution containing as many islands as exist in the electrical network. The minimum number of buses in an electrically isolated network in order to call it an island must be user-configurable.

b) Determine line and transformer overloads, voltage violations, and violations of generator and synchronous condenser VAr limits. Generator VAr limits shall be according to unit capability curves. Limits for non-telemetered quantities shall be user-enterable. It should be possible to sort the results based on line flows and or losses also.

c) Use injection measurements.

d) Use real time synchronized measurements phasor data (magnitude & phase angle) from PMUs with higher weight age and multiple voltage measurements from a single bus, including weighting to reflect the accuracy of the metering associated with each measurement.

e) Support pre-filtering of input data via data validity tests as defined in SCADA section, including the ability to recognize quality codes attached to the input data and to adjust the variances (sigma) or reject the data as appropriate

f) Detect bad data and measurement bias errors and cause a quality code to be set in the real-time database. Bad data detection shall be able to resolve multiple and interactive errors. It shall be possible for the programmer to disable and enable the setting of the quality code in the real-time data base on a global basis. A separate display should show the points where quality has been changed in SCADA

g) Assign the reference bus to the largest generating station by default. However, the operator must be able to change the reference, if desired.

h) Maintain bus voltages within high and low voltage limits on regulated buses in the unobservable portions of the network to the extent possible given the VAr resources available

i) Maintain generator and synchronous condenser VAr within high and low limits in the unobservable portions of the network

j) Handle the cases of reactive powers at a bus as listed below –

- Line Reactor MVAR should be taken care while doing state Estimation for MVAR of line

Algebraic sum of reactive power at a bus exclusive of reactive power of line reactors equals to Zero. If the line reactor is taken as bus reactor, the reactive power of the line to be taken into account for calculating bus mismatches.

Algebraic sum of reactive power at a bus including. reactive power of line reactors equals to Zero.

k) Accept injection, branch flow and voltage measurements in the unobservable portions of the network

l) Minimize observable-unobservable boundary flow mismatches without interference with the observable network solution

m) Assign generation, load and voltage values to any buses in the network

n) Estimate telemetered and un-telemetered tap positions for voltage transformers and phase-shifters

o) Calculate load power factor

p) Calculate and display a confidence factor based on the covariance of the residual of each measured quantity. Confidence factors shall be calculated each time the network topology or measurement set changes and shall be available for display and shall be stored in historian.

q) Allow operator control of the SE execution control parameters such as convergence tolerance and maximum number of iterations. A User Interface to automatically re-initialize the various parameters (operator selected) associated with State Estimation process after running a specified number of times by the operator shall be provided.

r) Allow the operator to enable-disable the use of telemetered values by the SE on an individual basis. Quality (including anomalous data quality) of the SCADA measurement should be visible for user to have the intuition for enable/disable the measurement.

s) Shall be able to rank the lines according to the losses and maintain the statistics of line losses for the line.

t) The user shall be able to specify the maximum, minimum and initial tap positions and step sizes for each tap-changing transformer and phase-shifter.

u) STATCOM reactive power limits shall be modelled as a function of the Voltage at the monitored Bus. Programmer-definable and user-selectable multiple curves shall be provided for each STATCOM unit.

2.2.8.3 SE Output Requirements

State Estimation output shall be for both the observable and unobservable portions of the entire network model and external power systems network. State Estimation output for the entire network model shall be as follows:

a) Vector voltage solution

b) Angle values with-respect-to the reference bus

c) Branch flows

d) Injections

e) Transmission loss for each branch and Area

f) The results of the State Estimation function shall be available for display in tabular form and also on SLD and Network diagram diagrams in the same formats as those used to display real-time data. These displays shall be generated automatically during preparation of SCADA displays and should not be prepared separately.

g) A dedicated display shall clearly identify the makeup of any islands that exist and show the status of all branches.

h) The user shall be able to save State Estimation solutions for use as base cases by the other PSA functions.

i) The user shall be able to save solutions in latest version (with backward compatibility) of IEEE format and PSS/E format.

j) The user shall be able to get the trend / profile of selected state estimated value on a curve and in a table.

k) A dedicated tabular display shall be provided to list the detected bad data.

l) A separate display shall be provided with listing of all loads and generators in cases where telemetry is rejected by State Estimator.

m) A separate tabular display with Each element (UNIT, REACTOR/CAPACITORS, BRANCH & Transformers) showing SCADA Measurement and corresponding Estimated Value.

n) The bus-symbolic view / bus-branch model/ node-breaker model of station to be auto generated from the Network database as per the modelling and connectivity to be made available station-wise for all elements for getting the various station-wise inputs and outputs of the EMS applications in a single view which in turn helps the operator in tuning of EMS applications in less time and more clarity.

o) Feature to save SE save cases for 13-month duration, which can be used for later on for study purpose. Historian sizing needs to be taken care to achieve this functionality.

p) Output of SE can be exported in any software format (.csv, .xls or .xml) and can be scheduled for automatic export periodically.

q) A display to be created for Node-Breaker model automatically for the station for rectification of node connectivity issues of the switching devices and elements.

r) A display of Bus-Branch model to be created automatically for the full network to have the topological connectivity indicating status of elements as Online/Offline/Open-ended branches (lines/xfmer).

2.2.8.4 SE performance metrics

The application must be able to display following parameters to evaluate SE performance

a. SE solution cost

b. SE convergence statistics over a day

c. Percentage telemetry availability for SE

d. Topology summary – No. of islands, buses, dead buses, observable buses

e. No. of units categorized as bad by SE

f. No. of loads categorized as bad by SE

g. Redundancy index of the system

h. Number of Observable/Unobservable Buses of the system

i. Percentage of Bad data measurements in the system

j. Total Installed capacity of the online Units in the Full Model.

k. Total MW Generation of the online Units in the Full Model. Total load and Generation of each Region along with its MW Interchange in the Model.

All these parameters must also be archived in the historian

2.2.8.5 SE displays

Following displays should be provided, but not limited to these types:-

a. Bus SE mismatch display

b. Bus measurement mismatch display

c. Breaker summary display Region-wise, Station-wise and Voltage-wise.

d. Sign flip display Region-wise, Station-wise and Voltage-wise.

e. Generation display (A list with all generators telemetered and estimated values)

f. Load display (A list with all loads telemetered and estimated values)

g. Island summary display

h. SE statistics and performance metrics display

i. Breaker anomaly display

j. Bad data detection display

k. Non telemetered points display.

l. Branch (Line and Transformer) Measurement Mismatch Display

m. Station Bus Summation of Active and Reactive Power for SCADA Measurement and Estimated Values should be displayed.

n. The application must also be able to give the list of points for which telemetry is not mapped.

2.2.9 Bus Load Forecast

The Bus Load Forecast (BLF) function shall calculate bus loads for the unobservable regions of the power system model using bus load distribution factors. The bus load distribution factors shall be applied to the total Control Centre load. Un-observability may be due to loss of telemetry or data exchange or insufficient telemetry.

Bus load distribution factors shall be maintained for every bus in the network model so that BLF can generate the bus loads used for line flow calculations by OPF (for example) and for pseudo measurement calculations by SE.

BLF shall calculate the busload distribution factors for all buses in the observable portion of the network and exponentially smooth them with previously calculated distribution factors to provide adaptive bus load distribution factors. Users shall be able to:

- Initialize and reset the dynamic factors from default or manually entered values, and
- Change the filter parameters used by the smoothing process.

Each bus load distribution factor shall express each conforming load as a function of the total Regional conforming load. Total Regional conforming load shall be the difference between "Total Regional Load" and "Total Regional Non-Conforming Load".
Provision shall be made for multiple sets of busload distribution factors. Sets shall be provided to cover:

a) Up to 4 seasons/ 4 calendar months of the year,
b) Up to five (05) different periods of the day, and
c) Up to seven (07) different day types; resulting in up to 140 sets. These sets shall be stored in Historian Server system.
d) Special day tagging of the day profile (cyclone, solar eclipse, earth hour etc.) to be available with retrieval.

2.2.10 Transmission Loss Sensitivity Factors

Transmission loss sensitivity factors shall be calculated by the Transmission Loss Sensitivity Factors (TLF) function. Sensitivity factors shall be used by any PSA function that needs to dispatch generation. The sensitivity factors for each source bus in the electrical network shall represent the sensitivity of system losses to changes in power injection at the bus. Real-time sensitivity factors shall be calculated considering parameters like HVDC set-point, transformer tap change, Generator reactive Capability and status of shunt reactors and MSR/MSC. The real-time set shall be calculated for immediate use by Power System Dispatching. User should be able to export the calculated loss sensitivities in the prescribed formats.

User shall be notified about change in dispatch schedule after running TLF function and optimizing the Transmission losses in the system.

Users shall be able to initialize and resets the sensitivity factors from default or manually entered values.

2.2.11 Network Sensitivity Applications

Line Outage Distribution Factors: The LODF value represents the fraction of the pre-contingent flow on a Branch (line and Transformer) that will be transferred to other Branch (line and Transformer) in the event of a forced outage of the Branch (line and Transformer). The LODF values should be available and displayed for any Branch (line and Transformer) w.r.t other branches defined by the user. It should be possible to define the Branch (line and Transformer) in the online database. Evaluation of these factors is very simple and efficient since these depend only on X matrix elements and line reactance. The application must be able to display the change on Branch (line and Transformer) for a particular Branch (line and Transformer) outage on the map board with the original as well as changes quantum visible with appropriate colors.

Generation Shift Distribution Factor: The GSDF value represents the fraction of the pre-contingent injection of the generator on all the lines in the event of the forced outage of a generator. The GSDF values should be available and displayed for any defined branch w.r.t the generators defined by the user. It should be possible to define the generators in the online database.

Load shift distribution Factor: The LSDF value represents the fraction of the pre-contingent drawl of a load on all the lines in the event of the forced outage of a generator. The LSDF values should be available for any defined generator defined by the user. It should be possible to define the loads in the online database.

The LODF, GSDF & LSDF values should be calculated after every valid or acceptable state estimator solution. A provision for defining the threshold for LODF, GSDF & LSDF values must be available to filter only the values above threshold.

The results of network sensitivity applications shall also be available on the network grid display in the following form:

1. User should be able to select the Network Sensitivity Application.

2. After selecting the appropriate NSA, a drop-down menu shall be automatically populated with related elements.

3. User shall be able to select the desired element as an input to NSA and all the results shall be displayed on the network grid display with the original values on lines and the change displayed adjacent to the original values. This information should be available in Tabular Display also

2.2.12 Contingency Analysis

The transmission system shall be periodically analyzed by the Contingency Analysis

(CA) function to predict potential problems if selected elements of the power system were to be out of service.

The CA function shall use the State Estimation results as a base-case and check specified contingency cases to determine if potential overloads or voltage problems through standard indices such as VCPI, L-index etc. exist. Functionality should be available to enable/disable base case violations to display as a solution for the contingency.

Performance statistics for CA to be available for Daily /Monthly/Yearly basis

2.2.12.1 Contingency Cases

Each contingency case shall consist of combinations of elements, including:

a) Branch outages
b) Reactor or capacitor switching
c) Generating unit outages
d) HVDC related equipment outages (poles, DC line, filters etc.) and sudden change in HVDC Power flow.
e) Load element outages
f) Switching device changes (open or close)

Following features are to be provided in contingency analysis:

a) Each case shall consist of the outage of up to multiple elements (at least 50) defined by the user interactively via display entry. It shall be possible for operator to select an element from single line/Network diagram (by clicking on it) for inclusion in a contingency case definition.
b) Each case shall be given a case number and be assigned to one of eight priority levels by the user. The user shall be able to designate the priority levels to be studied during each execution of CA.
c) The user shall be able to enable or inhibit the modelling of closed-loop control of transformer (voltage and phase-shifter) tap changers, reactor/capacitor switching and generating unit reactive power limiting.
d) In the event of generating unit outages or outages that cause a loss of load the change in generation/load shall be assigned to all remaining generating units/loads in proportion to its maximum capacity in the affected electrical island.
e) A complete solution shall be produced for outages that result in a change in network topology (such as the creation of new system buses or the merging of buses) or result in a group of buses being isolated from the rest of the system.

f) A complete solution shall be produced for each viable island (i.e. for each island in which there is a generation-load match within a predefined amount).

g) The operation of relay load changeover schemes shall be properly modelled. Such schemes automatically switch loads from a bus that is de-energized as a result of an outage to another predefined bus that remains energized.

h) Cascading outages shall be modelled. Operator will define selected branches as secondary outage devices. Each secondary outage device shall be associated with a secondary outage monitoring point. The programmer shall be able to specify that a unique limit be used as the MVA or MW limit for a monitoring point. If a secondary outage device's monitoring point violates an associated limit during evaluation of a contingency case, the device shall be added to the outaged elements.

i) There shall be up to 20 secondary outage devices. In those situations, in which secondary outage devices are added to the case, the output shall clearly describe the power system elements added.

j) The CA function shall study up to 250 contingency cases, including dynamically created cases. Dynamically created cases shall each consist of a single element taken in order of decreasing severity from the set of overloaded branches, if any, determined by State Estimation.

k) The limits used for evaluating violations shall be in MVA and Current. User shall be able to select from any of the above-mentioned three (03) types of limits.

l) Output of Contingency Analysis shall also be reflected in network displays (Geo Maps, SLDs etc.)

m) User shall able to create group of contingencies cases and define for must run for every execution of Contingency Analysis (CA)

2.2.12.2 Contingency Screening

The contingency cases shall be screened so that only those representing the most severe security problems need to be studied using full AC power flow techniques. Screening shall identify active and reactive power and voltage problems. The user shall be able to bypass the screening process by manually selecting specific cases for detailed analysis.

2.2.12.3 Full AC Analysis

After screening all contingency cases, full AC studies shall be performed on a user-chosen number of the most severe cases (up to 10).

CA shall contain violation checks for a user-specified set of branch flows and bus voltages, potentially all branch flows and bus voltages. Limits for non-telemetered quantities shall be the same as those specified for non-telemetered quantities for State Estimation Characteristics. In addition, for bus voltages, there shall be a set of limits on the deviation between the pre-contingency voltage and the post- contingency voltage at user specified buses.

2.2.12.4 CA Output

CA shall notify the user of each new contingency violation discovered. Overload conditions that exist in the base case shall not be alarmed unless they exceed the degree of overload in the base case by a programmer-enterable amount. CA output shall consist of the following:

a) For each element in violation, the output shall identify its name, the value of the parameter and its associated limit, and the value of the parameter in the base case.

b) CA output shall also include the base conditions of the outage equipment. Violations resulting from CA shall be ranked according to their severity in terms of either of branch flow or voltage flow violation or both (All 3 configuration shall be available in the application). An output summary shall be provided that lists the case number, case title, and priority for each case. The following information shall also be provided for each case:

   I. Whether or not the case was screened

   II. Result of screening, e.g., converged, diverged, split system, and inadequate generation

   III. Whether or not the screening indicated any potential violations

   IV. Ranking as the result of screening. This may include several numbers such as real, reactive, voltage magnitude, voltage deviation and angular separation based on user selected priority (top ten for each type of violations).

   V. Whether or not simulated with a full AC run

   VI. Results of simulation, e.g., converged with violations, converged without violations, and did not converge, diverged, severity index, previous severity index.

   VII. It shall be possible to display the results (Branch flow, Bus Voltages and angles) of CA on network diagram when full AC analysis is carried out.

2.2.13 Optimal Power Flow

An interactive Optimal Power Flow (OPF) shall compute active and reactive power flows and bus voltage magnitudes and angles for the power system model. The user shall be able to execute a power flow analysis only or an optimization analysis. OPF shall provide display-based input/output and shall include a load and generation scheduler. The Product should have facility for import and export of power System model files including following:

a) Generation Values
b) Load Values
c) Measurements
d) Transformer settings
e) HVDC set points
f) Generation Voltage Control values
g) Device states
h) MVAr values for shunt compensators

OPF shall execute as part of the real-time sequence and also in study mode. The user shall be able to restrict the optimization feature to the area of the model that is of interest by designating the control facilities which shall be eligible for adjustment.

2.2.13.1 General Characteristics

The following general characteristics shall be provided as a minimum:

a) The user shall be able to select standard Objective Functions with Control Functions as follows-
   - ➢ Objective Functions:
     - MW Loss Minimization
     - MVAR Loss Minimization
     - Economic Dispatch
     - Control Minimization
     - Feasible Solution
   - ➢ Control Functions:
     - Security Dispatch on user selected generators for control
     - Security Constraint Economic Dispatch on user selected generators for control
     - Transformer Tap Controls
     - Volt-VAR Controls
     - HVDC Setpoint Controls (Provision for regional loss minimization based on HVDC set-point)

b) User should be able to control convergence tolerances and other program parameters. The user shall be able to specify transaction schedules between each area with other areas. If the user fails to enter transaction schedules, then it shall be obtained for the appropriate times from the separate module of interchange scheduling applications.

c) Area interchange shall be computed by summing tie-line flows including Inter-Regional HVDC links at specified metering points. Either end of each tie line shall be able to be the metering point, including the opposite ends of two parallel tie lines.

d) Multiple power system viable islands shall be solved in a single program execution. Viable islands i.e., the islands in which the generation-load mismatch is less than a programmer-defined amount, must be solved even if other nonviable islands fail to converge. Non-viable islands, i.e., islands in which the generation load mismatch is greater than a tolerance, will be automatically deleted from the solution processing in order to ensure that the rest of the islands can be solved.

e) The user shall be able to specify the maximum, minimum and initial tap positions and step sizes for each tap-changing transformer and phase-shifter.

f) It shall be possible to freeze OLTC transformer taps and capacitors without need for element level control at their base case positions by a single user action.

g) The same sets of limits as specified in SCADA Limit Monitoring shall be used for overload and voltage monitoring. Option to change the limits shall be provided in the application.

h) The user shall be able specify the output of selected generating units. The user shall also be able to designate the start-up and shut down of selected units to be treated as OPF control variables.

i) The user shall be able to enable/disable load shedding on an individual bus basis, regional basis and state-wise basis.

j) The load shed limit for an individual bus shall be calculated as a user-definable percentage of the initial (base case) bus load. For example, for a setting of 25% and an initial bus load of 100 MW, OPF shall be able to shed up to 25 MW at the bus.

k) A bus voltage reset shall be possible via a single user action when running a change case from a solved power flow.

l) The user shall be able to disable generator reactive power limiting on user-selectable sets of units, e.g., on a Control Centre basis.

m) Phase Shifters control shall be available, and user can enable/disable the control as per requirement.

2.2.13.2 OPF Input Data

The user shall be able to specify the use of either saved base case as the input, initialize switching device statuses from either the real-time database or their normal status, and specify the use of power system device status values obtained from Outage Scheduler for a given date and time. The user shall be able to use any Generation Schedule listing also as input of Generator Loading.

The user shall be able to change any of the input data before requesting execution of the case. All input data shall be checked for reasonability and acceptable format when it is entered.

OPF function shall produce, at the option of the user, a Tabular Representation of the complete input data including the following:

a) Case description
b) Program parameters
c) Branch data
d) Bus data
e) Selection of objective function

2.2.13.3 OPF Output Data

OPF output shall be in engineering units (such as MW, MVAr, and kV) rather than per unit. The following output capability shall be provided:

- Output shall include bus identification, voltage magnitude in kV, and angle in degrees; MW, MVAr and MVA of all generators, loads and shunt devices, and MW & MVAr flows at each terminal of all branches.
- An interchange summary shall be provided showing desired and calculated net interchange, Total losses, generation, load, tie-line flows, bus mismatch, maximum bus mismatch, and spinning reserve.
- A generation summary shall be provided listing individual bus voltage, MW and MVAr, desired voltage, MVAr limits, and other controlled bus voltage data.
- An OLTC transformer summary shall be provided listing tap position, voltage, desired voltage, and maximum and minimum tap ratios.
- A summary shall list the solution diagnostics (such as MW and MVAr mismatches), tolerances, iterations, number of tap changes, total losses, total generation, total load and total number of branches.
- A summary shall list all buses where voltages are out-of-limits.
- An overloaded branch summary shall be provided.
- A load shed summary by bus and total by control area shall be provided.
- Title remarks of up to 600 characters shall be permitted at the beginning of each case.

- Output in latest version of PSS/E and IEEE formats (with backward compatibility) shall be available at the user's option.
- A summary shall list all the HVDC terminals and control recommendations.
- Output shall yield Sensitivity values corresponding to each control parameter as change in objective function value per unit change in control parameter.

2.2.13.4 OPF Base case

The capability to save 20 base cases on Auxiliary memory, Transfer base cases to and from archival media, and start from saved base cases shall be provided. It shall also be possible to use the results from the State Estimation to create a base case.

When the user wishes to use a stored base case as the starting point for an OPF analysis, a simple interactive procedure to recall the base case from storage shall be used. The user shall be able to change any of the base case data, such as breaker status, load level, or generating unit output, and execute an optimal power flow based on the revised input data.

2.2.13.5 Interactive Requirements

All input and output data shall be displayed on tabular displays and SLD & Network diagrams. The SLD & Network diagrams shall clearly identify the makeup of any islands that exist and show the status of all branches. The SLD & Network diagrams shall be essentially the same as those used for the real-time functions and State Estimation results. They shall include circuit breakers, and the user shall control the status of transmission lines by changing the status of the breakers associated with each line. All OPF input and output data shall also be available for printing at user request. The tabular displays shall be essentially the same as the printer listings.

Based on user-specified study date and time, the OPF function shall retrieve all available information about:

- User entered load,
- Generating unit availability from the Off-line Applications,
- Equipment outages from the Outage Scheduler,
- Bus load distribution factors from BLF.

2.2.13.6 Optimization Features - Security Enhancement

In addition to the standard power flow, which solves the power flow equation without regard to load bus voltage magnitude limits and branch power flow limits, a power flow shall be provided that optimizes a user selected function. The functions to be provided shall be active power cost, active power security, reactive power security, and losses.

Active power cost optimization shall minimize the cost of supplying active power. Controls available for use shall be generator active power output, parameter control of Flexible A.C. transmission system (FACT), TCSC, phase-shifter angles, import/export from other agencies, and DC line flows. These control variables shall be adjusted to achieve operating conditions that result in the minimum production cost. During optimization, limits shall be put on respective branch flows, bus voltages, interchange, spinning reserves, and control variables.

Active power security optimization shall shift the control variables, from their base case settings, the minimum amount required to satisfy operating constraints. Control variables and constraints shall be the same as for active power cost optimization with the addition of load shedding.

Reactive power security optimization shall shift the control variables, from their base case settings, the minimum amount required to satisfy operating constraints. Control variables shall be generator and synchronous condenser reactive power output, OLTC transformer tap positions, capacitor/reactor switches, continuous controlled variable reactors and SVCs. Constraints enforced shall be bus voltage limits, generator/condenser reactive power limits or MVA limit, reactive power branch flow limits, and control variable limits.

Loss minimization shall be used to minimize the active power losses for the control centre. Control variables for loss minimization shall be generator and synchronous condenser reactive power output, OLTC transformer tap positions, capacitor & reactor switches, DC line flows, continuous controlled variable reactors and SVCs. All control variable limits shall be respected. Other operating limits enforced shall be those associated with bus voltages and branch reactive power flows. Maximum angle violation shall also be considered as an operating limit during optimization process.

OPF shall include the following execution modes, each with its own objective function options and user-selection of constraints and control variables:

a) **Power Flow Mode:** Solves the power flow with no optimization.

b) **Real Power Security Mode:** Minimizes branch overloads by adjusting real power generation and load shedding.

c) **Real Power Cost Optimization Mode:** Minimizes total cost of power generation including losses.

d) **Voltage/Var Security Mode:** Minimizes voltage violations by adjusting reactive power resources and transformer taps.

2.2.14 Short Circuit Analysis (SCA)

The purpose of the short circuit Analysis function is to, periodically and on demand, compute the short circuit values for fault on selected system elements and throughout the network. The calculated short circuit values are to be compared against ratings for respective circuit breaker likely to be operated for clearing fault.

Since the topology and network parameters of the grid are fed into the system, a fault level at each node can be found out based on the Thevenin impedance at the node. The application should be able to output fault level of each node in the network.

2.2.14.1 Features & Interfaces

a) It should run in real-time as well as in study mode.

b) Shall be able to simulate Symmetrical and Unsymmetrical faults i.e. three phase fault (LLL), three phase to ground (LLLG), Phase to ground fault (LG), two phase faults (LL) and two-phase-to ground (LLG) fault.

c) Fault location can be selected on any of the network component i.e. bus-bar, generator bus, line etc.

d) Faults can be grouped. Specifying the group(s) of faults to be simulated.

e) The SCA shall interface with SE and get initial conditions i.e. positive sequence network configuration, parameters and pre-fault solution from SE.

f) In study mode SCA, the data shall come from Power Flow program.

g) It shall be possible to edit the current fault definition list or recover a default list.

h) Initialization shall be Cyclic and operator demand

i) Fault level of a bus / fault contribution from BUS and branches at 'N' levels away shall be available in MVA as well as kilo amps. (N is no of levels back for contribution output).

j) Fault level shall be available on single phase as well as three phase system.

2.2.14.2 Input/ Output Requirements

a) Number of faults (each type) simulated

b) Branch outages being simulated (if any)

c) Branch fault currents

d) Station and Node names along with post-fault bus voltages

e) Short circuit powers, currents and voltages calculated by SCA shall be displayed.

f) Ability to specify the number of nearby buses from the faulted bus and user selectable buses for output

g) Ability to specify the minimum amount of fault current in a branch for displaying it on output.

h) Real time Short circuit analysis shall issue alarm for a fault which produces a circuit breaker flow exceeding the maximum fault level.

i) **Pre-contingency and post-contingency fault levels for nodes:** Shall be calculated for contingencies and it shall be provided to sort the fault levels based on the difference in pre-and-post contingency fault levels.

2.2.15 Transmission Line/ Corridor Capability Monitor (TCM)

This application will run in real time and in study mode. The TCM application shall calculate Total Transfer Capability (TTC) and Available Transfer Capability (ATC) values for the defined pair of groups of nodes, corridors and Axis in the system.

Note:

- "Total Transfer Capability (TTC)" means the amount of electric power that can be transferred reliably over the inter-control area transmission system under a given set of operating conditions considering the effect of occurrence of the worst credible contingency.
- "Transmission Reliability Margin (TRM)" means the amount of margin kept in the total transfer capability necessary to ensure that the interconnected transmission network is secure under a reasonable range of uncertainties in the system conditions.
- "Available Transfer Capability (ATC)" means the transfer capability of the inter-control area transmission system available for scheduling commercial transactions in a specific direction, taking into account the network security. Mathematically, ATC is the Total Transfer Capability less Transmission Reliability Margin.

In Real time mode application shall use both SCADA values & state estimation result as base case to calculate TTC and ATC. Operator should be able to specify the Transmission Reliability Margin for any ATC calculation, such that TTC = ATC+TRM

In Study mode, application shall be able to calculate TTC and ATC at a given time in future. In study mode, application shall be initialized from its save case or from the save case of state estimator. These initialized conditions shall be modifiable by the user. The application shall take load data from interchange schedules outages schedules from offline applications & Outage Schedules from Outage Scheduler based on the study time.

- **TCM Input data**

The TCM function shall use the following:

(a) State Estimation results as a base case

(b) User shall be able to define multiple corridors for single base case. It shall be possible to increase/decrease load/generation for one or multiple corridors to get solutions for respective corridors.

(c) User shall be able to select branch (line/transformers) for a corridor from the network model database.

(d) User shall be able to save and retrieve the set of corridors defined under TCM application, whenever required.

(e) Day ahead inter-change schedules data from the scheduling program from offline applications

(f) Phasor data

- **TCM shall be limited to minimum of the following constraints:**

(a) Voltage limits

(b) Branch/ICT flow with multiple set of user configurable limits

(c) Angular pair limits

(d) **Peak-time Scenario (Defined by system operator)**

- **TCM output data shall be displayed on tabular and Network displays. Minimum following output capability shall be provided:**

(a) ATC

(b) TRM

(c) TTC

(d) Limiting constraint & violations

(e) Limiting element which is resulting into constraint

(f) Distribution factor of limiting constraint w.r.t. corridor under study.

(g) Angle Node pair values for all buses that exceed a user-entered limit for Angle difference.

The program shall be able to execute multiple contingencies set one by one and list out change in TTC for each contingency in the order of maximum TTC change. For each contingency, TCM output data shall be as listed above from (a) to (g).

The program should be able to get output by putting Availability schedule into OPF to find available transmission capability.

TTC/ATC calculation has to be n-1 compliant for multiple contingency sets from contingency analysis application highlighting TTC/ATC value with limiting constraints. For TTC/ATC application additional set of limits is required for assessment of the limiting constraints for elements for their selection to monitor for TTC/ATC application.

2.2.16 Dashboard for EMS Applications Output Assessment tool

Creation of a Dashboard for performance monitoring of EMS applications as per the sample attached at figure ***Appendix - B.*** The dashboard shall have following as a minimum:

a) It shall contain trend based on Boolean function to display the following:

State Estimator State (valid/invalid), Tolerable mismatch (% of Error Cost), weight convergence for valid solution, Status regarding Manual Triggering, etc.

b) It shall contain trends for the following:

Voltage convergence for valid solution, Percentage of Error Cost Mismatch Violations, Total generation, Total Load, Wind Generation, DC flow, frequency, Maximum Bus Mismatch, Maximum Bus Measurement Mismatch, Maximum Measurement Residuals, etc.

c) It shall also contain data for the following:

Total number of islands with indication of formation of new island(s), Total Voltage violations, Total Branch Violations, Unsolved contingencies, Total dead units, Total deadlines, Redundancy index, Total Buses, Total Dead buses, Units observable (number and %), Loads observable (number & %), Bus observability (number & %), Total Cost Index of the solution, Load Residual (real & reactive), Line Residual (real & reactive), Unit Residual (real & reactive), Transformer Residual (real & reactive), ZBR Residual (real & reactive), Bus Voltage Measurement Residual, etc.

EMS application Save cases, all applications output results and outage schedules shall keep on storing in historian system. User shall be able to easily retrieve this information from historian by selecting date/time range of Historian GUI.

2.3 Dispatcher Training Simulator

A Dispatcher Training Simulator (DTS) shall be provided for Control Centre computer system training during power system normal, emergency, restoration activities. The major DTS features shall include:

a) A Power System Model (PSM) that simulates the power system in a realistic manner, including its response to simulated events, Instructor actions, and Trainee actions. PSM response shall be identical to the response observed by the dispatcher in the actual computer system environment. The User Interface shall also be identical to that of the production system in order to provide a realistic and immersive training simulation.

b) A Hydro System Model (HSM) that simulates each hydro system in a realistic manner including reservoirs, rivers, flow control devices, and hydro power stations.

c) It shall model Renewable energy sources such as Wind generator and Solar model. The generator models of type 1, 2, 3, 4 and 5 must also be provided. Wind model detail is given in **Appendix M (2)**

d) Power Plant Controller to be modelled for Wind/Solar Generator.

e) A Model that adapts to provide an exact representation of the New Control Center. It shall consist of dedicated hardware so that training for operators can be conducted without disturbing Control Centre's real-time operations

f) An approach that allows any real-time console or device to be assigned to the DTS for its use, and vice-versa. The consoles shall be assignable as trainee or instructor consoles. The DTS shall support single or multiple instructors.

g) **Trainee or instructor consoles. The DTS shall support single or multiple instructors. It shall include** Instructor control features that include the ability to set up, control, participate in, and review the results of a training session.

h) An ability to obtain data from the SCADA/EMS systems automatically for DTS initialization. The initialization data shall include real-time snapshot, SE save cases and interchange schedules. While initializing from real time, there must be an option to assign participation factors of loads in SE as participation factors of loads in DTS application and this participation must remain the same in that instance of DTS.

i) A design that prevents actions performed by the Instructor and Trainee using the DTS from affecting the real-time system database or the actual power system.

j) An ability to simulate actual system disturbances from "State Estimator Solution" and from "historical data snapshots" stored by the Real-Time Database Snapshot function.

k) An ability to establish the following training conditions as a minimum:

(a) Normal steady-state
(b) Generation control
(c) Transmission control
(d) Demand control
(e) Load shedding
(f) Substation control
(g) Heavy load
(h) Line, transformer, and tie-line overloads
(i) Low voltage
(j) Light load
(k) High voltage
(l) Minimum load (excess generation)
(m) System disturbance
(n) Loss of major units
(o) Loss of multiple tie lines
(p) Loss of major transmission lines

(q) System islanding
(r) Voltage collapse scenario
(s) System blackout
(t) System restoration including black start

2.3.1 Power System Model

PSM shall include:

a) The power system network, generation, and loads of controlled area as envisaged in the specification and portions of its neighboring system

b) Means for the Instructor to perform the functions normally handled by operations personnel at substation, power station, Control Centre, and other locations in support of a particular EMS/SCADA computer system,

c) A simulation of the interface between the EMS/SCADA computer system and the equipment that is monitored and controlled by this system.

PSM shall be valid for normal, emergency, and restorative conditions, including a frequency range of 48.5 Hz to 51.5 Hz, voltages of 0.70 to 1.30 per unit, and any conditions in which the power system being modelled is stable.

PSM shall be capable of simulating conditions in which up to at least 10 electrical islands exist, each with its own frequency. Island blackouts shall be supported such that the collapse of any island shall not cause the entire simulation to abort. When islanding or island blackout occurs, error messages shall be displayed to the Instructor that describe the cause of islanding or blackout, and the power system operations functions shall continue to perform for the Trainee in the same fashion as they would if the same situation occurred in the real-time system.

The ability to simulate unit start-up and restoration of one or more totally blacked out islands shall be provided. This shall include reconnection of energized islands via circuit breakers, subject to supervision by appropriate relay models. It shall be possible to bypass synchro-check relay models say by way of alternative supervisory control points.

The DTS shall include default values for all model parameters in places where Employer/Owner chooses to use generic models for elements such as generating units rather than using models of specific units.

a) Load Modelling:

PSM shall model both active and reactive power loads in the power system. The load shall consist of three components: conforming, non-conforming, and random.

The conforming portion of the active power load shall be based on stored load curves. Each load curve shall represent a profile of the load over 24 hours using straight line segments for each five-minute period. The ability to use separate load curves for SLDC power system, Regional Power System and each external power system included in PSM shall be provided.

The load curves shall be stored in normalized form and shall require a peak load to be specified for all separate power systems being modelled. It shall be possible to use the same load curve for the separate systems, each of which may have a different peak load. System should have functionality of saving/using load curves for different seasons and day of the week (Including holidays)

The Instructor shall be able to retrieve load data and build a DTS load curve. The Instructor shall examine the stored load data and then select the desired data. The DTS functions shall translate the selected data into the form required for a DTS load curve.

The conforming active load shall be distributed to the load buses using Instructor-selectable and modifiable sets of distribution factors from the Bus Load Forecast function. The reactive part of the conforming bus load shall be a percentage of the corresponding active power load.

The non-conforming part of each bus load shall be a time-varying set of active and reactive power values with fifteen-minute resolution. The random component of load shall consist of a random variation that follows a uniform probability distribution applied to each load.

The load model shall also include the following features:

a) Curtailable load schedules
b) Load shedding and restoration by under frequency relaying and supervisory control
c) Effect of cold load pickup on load restoration
d) Load variation as a function of island frequency with programmer-adjustable load versus frequency parameters for each load
e) Load variation as a function of bus voltage.

b) Energy Source and Frequency Models:

Energy sources shall be modelled in the DTS, including fossil steam, nuclear steam, hydroelectric, combustion turbine, combined cycle generating units, solar and wind. Each energy source model shall include a governor load reference model, a governor model, and a turbine model.

The Instructor shall be able to enable/disable (block) governor action on an individual unit basis. The ability to include the steady state effects of automatic voltage regulators (AVRs) and power system stabilizers (PSS) shall be provided.

Models of varying complexity shall be provided for all types of conventional units. The high-level models, which are the most complex, shall be represented with high accuracy; high computation models and includes all details of boiler turbine and other auxiliaries. The other models shall be fast computing approximate models and shall represent various units by changing its parameters. In general, the model shall be in accordance with IEEE standard.

The frequency in each island of the power system shall be modelled as a function of the island power mismatch, inertias, and sensitivity of the island load to frequency.

c) Power System Network Simulation:

The DTS shall include a model of the power system network that is consistent with that used by Control Centre's power system operations functions. The model shall include:

a) Steady state models with appropriate dynamic time delays for automatic tap changing (including phase-shift) transformers. Provision to enable or disable the automatic tap changing feature by the user should exist.

b) Automatic control of Var resources such as capacitor/reactor devices, static Var compensators, generators, and synchronous condensers.

c) Time-varying models of HVDC systems consisting of values of the active power flow on the DC line as a constant, or target with an operator-selectable ramp rate. The reactive requirement of the convertors shall be continually calculated as a function of the active power flow. Reactive compensation shall be automatically switched depending on RPC operating and control modes, based on the latest practices and trends being followed.

d) Instructor ability to perform any of the functions normally performed by operations personnel at locations remote from the Control Centre computer system that in its DTS form is being used by the Trainee. For example, it shall be possible for the Instructor to act as a plant operator by placing generating units on and off line and by changing unit power outputs and limits. The Instructor shall also be able to simulate supervisory control of switching devices and to enter interchange schedules.

e) Models for the following types of protective relays- It shall be possible for the Instructor to inhibit and enable the functioning of each relay model individually via displays. There shall be a timer associated with each relay model that is started when the input conditions (under voltage, under frequency, etc.) are satisfied. The relay output shall not occur until after the timer has timed-out. The time delay shall be specified separately for each relay model over a range of zero seconds to 10 minutes in 10 second increments.

   The operation of a relay shall result in the initiation of one or more Instructor specified events. The event(s) associated with a relay's operation shall not be restricted to the substation in which the relay is located, so that transfer-trip operations may be simulated.

- **Directional and Non-Directional IDMT:** These shall be used to operate breakers at specified Current and time delays.
- **Under/Over frequency:** These shall be used to trip load and generation at specified frequency levels.
- **Under/Overvoltage:** These shall be used to operate breakers at specified voltage levels.
- **Synchro-check:** These shall be used to inhibit the closure of circuit breakers if the voltage and phase angle are not within limits when the two ends of the breaker are in the same island, or if the voltage and frequency are not within limits when the two ends of the breaker are in different islands.
- **Automatic Reclosure:** This feature shall be modelled to attempt the Reclosure of breakers tripped due to the operation of another relay. These relays shall be modelled with up to three Reclosure per relay, each with a separate Instructor-enterable delay.
- **Time Switched:** These shall be modelled to operate according to a pre-specified time program.
- Over Current Operation
- Distance Protection Operation
- Local Breaker Backup (LBB) operation
- Switch On To Fall (SOTF) Operation

f) **Branch fault simulation:** The Instructor shall be able to specify a fault by indicating the time of its occurrence, its location, and its duration. At the proper time the DTS shall open all switching devices that are supervised by protective relays and that are necessary to clear the fault. Should any of the switching devices necessary to clear the fault fail to operate, because it has a stuck breaker event enabled, the device shall not operate and the designated back-up devices shall operate instead. Should the Trainee or Instructor attempt to reclose any of these devices while the fault still exists, i.e., before the specified fault duration has expired, the device shall trip again. If the Trainee or Instructor should isolate the fault using sectionalizing switches, reclose the devices that cleared the fault, and then attempt to reclose the sectionalizing devices while the fault still exists, the DTS shall clear the fault in the same manner as it cleared the fault initially. Branch fault simulation shall be carried out using events and event groups, Sectionalizer, re-closure etc. are to be modelled only to the extent they are included in the SCADA system.

g) All measurements and device conditions collected by the EMS/SCADA computer system for which training is being conducted. This shall include measurements from RTUs, local I/O, and data exchange links.

h) Accurate models of all devices in the power system that are under supervisory control by the computer system for which training is being conducted. The simulator shall accept control signals generated by the Model, respond in a manner analogous to the actual device, produce the output signals necessary for the network model, and produce the output signals normally monitored by RTU, local I/O, and data exchange software.

i) Accurate models of all devices in the power system that are controlled by local controllers. The model shall include the device and its controller. For example, PSM shall model tap changing transformers with local control loops, static Var compensators, and capacitor banks that control a local bus voltage.

j) User Defined models that can be built from smaller logical blocks (such as low pass filter, high pass filter, differentiator block, integrator block, band pass, band reject filters etd) to simulate the performance of power electronic devices or other non-standard models of equipment such as AVR/PSS etc

d) External Generation Control:

Models of generation dispatch and control operations for areas external to the Control Centre's Model shall be provided. These models shall emulate operations in the Control Centre's region. The models shall contain all of the features of the vendor's standard approach and shall include:

a) The ability to model generating units in external areas

b) The ability to schedule interchanges transactions between the Control Centre's Model and external areas

2.3.2 Hydro System Model

HSM shall represent the various hydro systems, including turbines, reservoirs, flow control devices, and inflows. HSM shall include a representation of mechanisms that allow personnel other than the Control Centre computer system user to affect the hydro system plus a simulation of the hydro equipment the Control Centre computer system monitors and controls. HSM shall include the ability to compute:

a) Streams and other inflows as a function of time

b) Reservoir contents as a function of inflows and outflows and elevations as a function of reservoir content

c) Hydro-electric power output as a function of head and the number of units connected to a common tunnel or penstock

d) Flows through flow control devices as a function of water level and device opening

e) Spills as a function of water level and, where appropriate, gate opening

f) Water levels controlled by siphons and pumps

g) Transportation delays.

2.3.3 DTS Model

DTS model shall be capable of representing the EMS/SCADA **applications including AGC (excluding Load forecasting & DSA)** for which operators are being trained. It shall consist of an exact replica of a Owner-designated subset of the hardware used in the SCADA/EMS Control Centre computer system and the same software used in the Control Centre computer system with modifications necessary to interface with PSM and HSM.

DTS Model shall duplicate the Control Centre computer system from the perspective of the Trainee interacting with the DTS from the training console. In this respect, the following functions shall be included in the DTS:

a) Data Acquisition and Supervisory Control

b) Scheduling Functions

c) Operations Monitor

d) Power System Analysis

e) User Interface

The functions shall be copies of the corresponding functions in the real-time Control centre computer system with the exception of those functions such as:

a) SCADA that interacts with the actual power system,

b) Data Exchange that interacts with other computer systems, Differences between these functions and the corresponding functions in the Control Centre computer systems shall be limited to those changes required for interaction with PSM and HSM.

Functional differences apparent to the Trainee are not acceptable.

2.3.4 Instructor Control

The Instructor shall be able to perform pre-session, session, and post-session activities. The tasks performed by the Instructor shall be supported by one or more consoles that shall include all the capabilities of the Trainee's console and additional instructional capabilities.

Each training session shall consist of executing a scenario (tailored to the simulated Control Centre computer system) starting from a base case. The base case shall consist of a solved network output case from the state estimator or power flow and one or more load curves. The scenario shall consist of one or more event groups each of which consists of one or more events.

Pre-session activities consist of scenario building and development of events that occur during the training scenario. A power flow function shall be provided in the DTS to support this feature.

Session activities performed by the Instructor include initiation, control, and participation in the training session.

Post-session activities consist of session review and evaluation of Trainee performance. The DTS shall maintain records of the training session so that the base case, scenario, Trainee actions, and other session activities may be reviewed.

1. **Pre-session activities:**

The Instructor shall be able to create a base case and to execute a power flow if desired to initialize the base case. The Instructor shall be able to build groups of events scheduled to occur during the training session. A training session shall be built by combining one or more event groups with a base case.

- **Scenario Construction:**

The following features shall be provided for building a training session which allows the instructor to:

a) **Base Case Construction:** Set conditions, parameters, and limitation for equipment in the network database. It shall be possible to initialize a base case from the following sources:
   a) A stored base case created in the DTS
   b) A power flow solution obtained in the DTS
   c) A power flow or State Estimation solution obtained from the EMS/SCADA system via local area network services.
b) **Base Case Store:** Save a base case for future use. It shall be possible to transfer saved base cases to auxiliary memory (e.g., magnetic tape) and to reload saved base cases from auxiliary memory.
c) **Base Case Select:** Select a specific base case for modification or further processing. Base case selection may be indexed by title or subject.
d) **Base Case Review:** Display the contents of the base case.
e) **Base Case Editing:** Modify a base case and to store the updated version.
f) **Event Group Construction:** Construct event groups containing one or multiple events. The Instructor shall be able to define the events within the event group to occur simultaneously or according to other parameters of time or system conditions. Checks shall be performed to assure that each event entered is one of the predefined set of events and that the equipment and parameters associated with the event are valid and complete for the event specified.
   The system shall provide an interactive means for specifying the device or

point associated with each event.

g) **Event Group Store:** Save the event group constructed for future use.

h) Event Group Select: Select one or more event groups for incorporation into a training scenario.

i) **Event Group Review:** Display events within an event group.

j) **Event Group Editing:** Modify an existing event group and to store the updated version.

- **Event Types:**

The Instructor shall be provided with a set of permissible event types that can be scheduled as part of a scenario. As a minimum, the following event types shall be included:

a) Total or partial loss of generating unit output

b) Change of bus load

c) Change of system load

d) Change of scheduled interchange transaction

e) Change of voltage schedule at regulated bus

f) Fault application on specified bus for specified time duration

g) Circuit breaker trip/close

h) Circuit breaker trip with successful re-closure

i) Circuit breaker trip with unsuccessful re-closure

j) Supervisory control disable/enable for specific device

k) Stuck breaker enable/disable for breaker associated with up to ten other breakers controlled by breaker failure relaying. Event and Event groups can be used to simulate this scenario.

l) Relay status enable/disable

m) Loss of RTU due to telemetry failure for specified period of time

n) Loss of single RTU point

o) Replace value of telemetered point

p) Messages to Instructor

q) Pause simulation

r) Demand snapshot

s) DC line fault-on VSC as well as LCC HVDC lines

t) Faults/Oscillations near HVDC AC terminals leading to disturbance in HVDC system.

u) Faults/Line tripping near the solar and wind parks leading to LVRT/HVRT operation.

- **Event Initiation:**

Events shall be executed at an Instructor-specified time, when Instructor-specified conditions occur, upon Instructor demand, and when protective relays operate. Event initiation shall include:

a) **Time Dependent Events:** These events shall be scheduled by the Instructor to occur at a specified simulated clock time or at time intervals relative to the start time of the scenario.
b) **Conditional Events:** Conditional events shall be based on simulated power system conditions obtained from PSM and HSM. The Instructor shall be able to specify a conditional event by specifying a permissible event (see above) and a Boolean equation for the power system condition that will trigger the event. The Boolean equation shall allow the following triggers to be incorporated separately or in combination:
    - A status variable equal to a defined state
    - An analog variable above or below a defined threshold
    - Change in analog variable from one DTS cycle to the next by more than a defined amount (positive or negative).
c) **Probabilistic Events:** The instructor shall be able to define an event within a given time interval with a pre-defined probability. Such as there is a 25 percent chance that a load point will increase by 100 MW during the specified time window.
d) **Demand Events:** The Instructor shall be able to demand the immediate execution of an event without having to insert it in the events list.
e) **Relay Initiated:** The operation of a relay shall result in the execution of one or more Instructor-specified events.

2. **Session Activities:**

The Instructor shall be able to monitor the training scenario and guide it toward a specific objective by inserting new events omitting scheduled events, and performing other actions. The following commands shall be provided to control a Trainee scenario:

a) **Pause/Resume:** Allows the Instructor to suspend or resume the training scenario without affecting the scenario. While in the Pause mode, the Trainee and Instructor shall be able to call all displays but perform no other functions. The Resume command shall resume the simulation from the point at which the pause occurred.
b) **Slow Forward (Power System Model only):** Allows the Instructor to move a training scenario forward at an Instructor-specified speed slower than real-time.

c) **Event Insertion:** Allows the Instructor to add new events when a training scenario is in progress without the need to interrupt the training scenario.
d) **Event Demand:** Allows the Instructor to demand the immediate execution of an event.
e) **Event Omission:** Allows the Instructor to omit a scheduled event from the training scenario in progress without interrupting the training scenario.
f) **Periodic Snapshot:** Allows the Instructor to create a historical file that is periodically updated with session data necessary to resume simulation as it occurs during the simulation. The DTS shall not pause while the snapshots are being collected and saved. The snapshot save area shall be circular in nature where the oldest snapshot will be overwritten each time a new snapshot is saved when the save area is full.
g) **Demand Snapshot:** Allows the Instructor to create a historical file, identical to that created by a periodic snapshot, on demand during the simulation. The DTS shall not pause while the snapshots are being collected and saved.

3. **Post-session Activities:**

The DTS shall provide the following capabilities to assist the Instructor in reviewing a training session with the Trainee:

a) **Snapshot Review:** Initialize the DTS with a snapshot saved during a training session. After a snapshot has been loaded, the Trainee and Instructor shall be able to call displays to examine any data normally available during a session.
b) **Snapshot Resume:** Resumes the simulation from a snapshot in the same manner as it would resume from a Pause.

2.3.5 General Requirements

General DTS requirements are presented in the following sections.

2.3.5.1 DTS Performance and Sizing

The DTS network model solution shall be updated at an average rate of three seconds. For one base case power flow and two further power flow solutions needed in case of cascading contingencies, the network model solution update period shall not exceed five (05) seconds.

Dynamic equations for the energy source and frequency models shall be solved using a time step of one second or less. The performance requirements for the Control Centre Model functions shall be identical to those of the corresponding Control Centre computer system functions.

The DTS shall be sized the same in all respects as the EMS/SCADA real-time computer system. In addition, the capabilities of the DTS shall include the following items for Control Centre computer system that is simulated:

a) 125 load curves
b) 20 DTS base cases
c) 20 scenarios
d) 250 event groups
e) 50 events per group
f) 35 session snapshots
g) 5-minute snapshot periodicity
h) 125 conditional events
i) 15 terms per conditional event
j) 1,000 variables in conditional events

2.3.5.2 DTS Database and Displays

The DTS database shall be generated from source data obtained from the Control Centre SCADA/EMS systems. When the DTS database is generated, it shall use as much of the source data as necessary for its purposes. When source data is generated, it shall contain only one copy of a data item even if it is in both databases.

Thus, items such as point descriptions, unit characteristics, and branch impedances shall be entered once and transferred into both databases. When a new database is built for the DTS, saved base cases and event groups based on the old database shall not be destroyed or invalidated unless directed by the programmer.

The network model used in PSM shall be based on the network models used by the Power System Analysis functions in the real-time Control Centre computer systems and any modification thereof.

There shall be only one description of display formats and one set of display linkages for displays that are common to the Control Centre computer systems and the DTS. All Control Centre Computer system displays shall be directly useable in the DTS. DTS displays shall be distinguishable from Control Centre computer system displays by the use of a unique background color or other display attribute approved by Employer. Suitable provision shall be made to prohibit the use of control centre computer system displays background in the DTS environment.

2.4 Automatic Generation Control (AGC)

Introduction:

Employer/Owner intends to implement Automatic Generation Control (AGC). Pan India AGC with all 5 regions and constituents within it could be considered as one control area with user flexibility to spilt/merge control areas. Each regional/state/constituents entity power station within its jurisdiction is a control area by itself. Split/Merging of control area should be user dependent without any limitation on creation of number of new control areas. Each of the neighbouring country power system interconnected with the National Grid shall be defined as another control area for defining the trans-national exchanges. The ACE calculations, performance monitoring etc. shall be carried out for region and each constituent's (control area) within it. However, gradually this can be extended to Bid Area or each regional entity as one control area. The complete AGC system shall be implemented in two parts.

In the first part, the AGC system will be running at RLDCs/SLDCs SCADA/EMS system to control frequency and interchange with the control area. The contractor shall provide the AGC system at RLDCs/SLDCs meeting the functional requirement as described in subsequent sections. The AGC system at RLDCs/SLDCs shall be able to transmit the MW set points signals to the entity generators (plant wise) for increase /decrease of generation from their scheduled generation.

In the Second part, all the Entity Generators identified for providing secondary control through AGC, shall have AGC servers installed in their premises. The AGC system installed at entity generators, will receive the MW set points for the station as a whole, and do further distribution among the physical generating units within the station considering the technical minimum/maximum, ramp up/ramp down rate, etc.

The present scope of work for the contractor is to design, engineering, installation, commissioning and testing of AGC system (first part only) as per the signal list mentioned in **Part B Appendix L.**

User Interface Requirement as described in Section 3, Part B of this Technical Specification shall be provided for all the AGC functions as mentioned in the following sections.

***"*Contractor's Standard Product"**

Bidders are encouraged to supply standard, unmodified products that meet or exceed the Specification requirements. These products may be provided from the bidder's in-house baseline offerings. Alternatively, they may be provided by the computer manufacturer and established third-party software suppliers. Bidders shall describe all standard; unmodified products proposed and shall highlight those features that exceed the Specification requirements. Although the bidder is encouraged to use as much standard hardware and software as possible, the proposal will be judged by its conformance to the functional requirement of Specification. The proposal shall clearly identify all deviations from the Specification to help Employer/Owner evaluate the degree of conformance of the Bidder's offering."

2.4.1 Generation Control

The principal Generation Control functions described herein include:

- Operations Monitor (OM)
- Automatic Generation Control (AGC)

- Reserve Monitoring (RM)

These functions address the RLDC/SLDCs operational objective of Reliable Power System Operation. These functions shall monitor and coordinate generation while supporting state, regional and national LDC operating personnel. Although the Generation Control functions, specifically AGC, will execute in close-loop and, the Contractor shall provide the software, database, and user interface to perform closed-loop generation control. The user shall be able to test and activate AGC in a closed-loop mode as control equipment becomes available in the field.

Generation Control shall assist the RLDCs/SLDCs dispatchers as hierarchal control to maintain scheduled frequency and scheduled power interchanges by:

(1) Running the power stations within their control according to RLDC/SLDC schedule

(2) Allocating the generation raise/ lower signal within each RLDC's/SLDC's area of jurisdiction

(3) Using available generation to maintain power system frequency

(4) Monitoring available Up and Down spinning and non-spinning reserve capacities.

Within this context, the principle real-time dispatching activities of the LDC are summarized as follows:

Activities:

- Monitor the Control Areas generating resources, reserves, loads, inter-regional and inter-state imports/exports, and frequency
- Monitor each Control Area's actual net interchange versus its scheduled value (obligation) and maintain records of interchange errors
- Dispatch the power stations within respective control area.
- Enter into import/export transactions with other control areas.
- Archival of the telemetered and calculated signals as per, but not limited to, user defined signal lists in the historian at a configurable periodicity.

2.4.1.1 Operations Monitor

Operations Monitor (OM) shall provide shift operators/supervisors with a continual and accurate description of the demand/supply situation within their areas of responsibility. OM shall produce information for display (numerical and trending) and for historical records. All the items listed below shall be calculated and monitored at the RLDC/SLDC, which shall receive the required telemetered, calculated as well as user-entered information from all relevant sources comprising the hierarchical SCADA/EMS.

The following calculations as a minimum shall be performed at an adjustable periodicity (initially set to 1 minute; minimum configurable periodicity shall be 2 second) and shall consider quality of every signal:

(a) Actual Generation MW:

(1) Total for all India

(2) Total for each control area

(3) Total for each company/part of company, power stations, regional/state entity and the users' share breakdown.

(4) Total number of plants in remote along with MW capacity in remote for monitoring Installed Capacity.

Generation shall be mentioned fuel-wise also.

(b) Spinning Reserve MW:

(1) Total for all India

(2) Total for each control area.

(3) Total for each Company/part of company, power stations, regional entity and user.

(4) Total for Cross Border, International (as applicable).

(5) Up and Down Spinning reserves calculation by the following-

Up Reserves -

$$Up\_Reserve = Min\ of \{(In\_effect\_Regulating\_limit_{\ High} - Actual_{Plant/Unit}), Ramp\_Rate\}$$

Down Reserves -

$$Down\_Reserve = Min\ of \{(Actual_{Plant/Unit} - In\_effect\_Regulating\_limit_{\ Low}), Ramp\_Rate\}$$

I. With CB Status only

II. With both CB Status and Local/Remote Status

(6) Cold Reserve Calculation

$$Cold\_Reserve = Installed\_Capacity_{without\_considering\_CB} - Installed\_Capacity_{with\_considering\_CB}$$

Unallocated Generation shall be mentioned fuel-wise also.

(c) AGC Despatchable Margin Calculation

Up Margin

$$Up\_Margin = \left(In\_effect\_Regulating\_limit_{\ High} - AGC\ Setpoint_{Plant/Unit}\right)$$

Down Margin

$$Down\_Margin = \left(AGC\ Setpoint_{Plant/Unit} - In\_effect\_Regulating\_limit_{\ Low}\right)$$

I. With both CB Status and Local/Remote Status

(d) Net Interchange MW (actual, scheduled, and deviation from schedule): Net Interchange definitions and calculations shall be user-definable:

(1) Net for all India and breakdown per region and control area.

(e) Actual Drawl MW (including transmission losses):

(1) Total for all India

(2) Total for each control area.

(3) Total for regional/state entities.

(4) Total for Inter-national.

(f) Area Control Error (ACE): ACE for operating (5-Five Regions and constituents within each Regions) and processed ACE values shall be calculated based on actual frequency, actual net interchange (regional/state and constituents), scheduled frequency, and scheduled net interchange. Control areas and associated ACE calculations will be defined by Employer/Owner during project implementation. Flexibility to create new control areas shall be provided.

(1) For all India

(2) For each control area.

The RLDC/SLDC shall retain the operational characteristics of each power station's generating unit within its jurisdiction. The RLDCs/SLDCs shall report changes to unit characteristics to the RLDCs/SLDCs as they occur. Each RLDC/SLDCs shall maintain its own unit information.

2.4.1.2 Automatic Generation Control Functions

The primary objective is that AGC shall provide supplementary or secondary control action, which attempts to maintain the steady state values at specific levels. Primary control action for short-term swings shall be provided by the governors of the unit prime movers. The primary purpose of AGC to be delivered under this project is to adjust generation in response to changes in area load and Interchange requirement and to return frequency to its original value and maintain the difference between the constant frequency control error and the constant net interchange error within an acceptable range. This difference is the Area Control Error or ACE.

Automatic Generation Control (AGC) shall have the ability to:

(a) Execute in open-loop, i.e., without sending control signals to the generating units

(b) Perform standard load-frequency control calculations if the generating capacity exceeds the load requirements, i.e., maintain scheduled frequency and net interchanges within prescribed values.

Full capability shall be provided for the AGC functions to be field-upgradable to closed-loop operation without any need of additional computer software and/or hardware if, at a later date, Employer/Owner chooses to do so.

RLDC/SLDCs dispatchers shall be provided with the ability to manually select either the Load Frequency Control (LFC) Mode or Tie Line bias. AGC shall compute the desired MW increase or decrease at each generating unit. The required MW changes shall be required to be sent plant-wise or unit-wise as per the requirement of the Employer/owner on the case-to-case basis. The software shall be capable to model and integrate signals from different types of power plants such as thermal, hydro, open cycle gas turbine, combined cycle gas turbine, pumped hydro, Battery Energy Storage System (BESS), solar, electrolyser, etc. The software shall have necessary features by default to handle specific requirements of the different types of power plants. For example, the BESS model shall be capable of handling State Of Charge (SOC) requirements and any other conditions specific to BESS.

Thermal Plant's Setpoint need to be sent plant-wise and hydro plant's setpoint need to be sent unit-wise (especially for Francis turbine to take care of prohibited zones). The dispatcher shall be provided with the ability to validate or manually modify the MW changes required at each generating unit and power station. Upon dispatcher request, the MW change requirements shall be sent to the power station operators for subsequent control action.

During periods characterized by low frequency and generation capacity deficiency, AGC shall compute the amount of MW load reduction to be implemented. This information shall be displayed/ sent at the LDCs and, in addition, shall be automatically made available as input to the SCADA and ICCP.

At the RLDC/SLDCs, the Generation Control applications shall be fully implemented to allow the dispatchers to maintain the scheduled frequency and net interchanges within the prescribed limits. At the RLDC/SLDCs the capability shall be provided for the dispatcher to monitor the execution of the Generation Control applications within the RLDCs/SLDCs through periodically and on-demand updated Generation/Load Summary displays. Data for each generating unit region wise shall be displayed.

AGC shall retrieves and processes SCADA data and also trigger the rest of the AGC sequence, which shall be user configurable, which includes:

- ACE calculations
- Issue of controls
- Reserve Monitor

AGC shall be capable of providing supplementary control that automatically adjusts the power output levels of identified generators within the defined control area in response to Area Control Error. AGC shall account for the number of generating units and tie lines within a control area. Automatic Generation Control (AGC) shall have the ability to (through simple graphical user interface):

(a) Select/ Modify the AGC Status of operation

System Operator/User shall be able to select or modify one of the following AGC Status, either:

a. ON —AGC is fully functional and control command are issued.

[This will be enabled once the AGC system at Regional/State Entity Generators is in service]

b. OFF — Off Control. AGC is not functional, but issues Suspend status to power plants.

c. MONITOR — Monitor Control. AGC is fully functional, except no controls are issued (i.e., Monitor only). Shall issue suspend status to power plants.

On Selection the new status shall become active, next AGC cycle.

(b) Select the type of computation for ACE (tie-line bias control, frequency control only, or tie-line control only)

Three types of dispatcher selectable ACE calculation procedures shall be provided as follows:

The total plant allocation action required in AGC's control cycle shall be determined at the RLDC/SLDCs and assignments made to individual plants and units based on their control and operating status, operating limits, response rate limits, and deviation from schedule/ desired loading. Plants and unit control modes shall initially be set by default to "Off Control." Their limits, however, shall be dispatcher selectable and the capability shall be provided to adjust the parameters of AGC through user interface. The plant allocation function shall continuously determine MW requirements for plants under RLDC/SLDCs jurisdiction.

Three types of dispatcher selectable ACE calculation procedures shall be provided as follows:

(a) **Tie-Line Bias Control**, where ACE is calculated from the following formula:

ACE = $(I_a - I_s) - 10\, B_f\, (f_a - f_s)$+Offset

where:

ACE = positive value for excess generation

I_a = Actual net interchange for Regions and States (positive value for export)

I_s = Scheduled net interchange for Regions and States (positive value for export)

B_f = Frequency bias coefficient in MW/0.1 Hz (negative value)

f_a = Actual system frequency

f_s = Scheduled system/reference frequency with an ability to change the reference by user (e.g. 50Hz to be changed as 49.97Hz) on the fly.

Offset = Provision for compensating errors such as measurement error; default value zero.

(b) **Frequency Control only**, where ACE is calculated by setting $(I_a - I_s)$ to zero

(c) **Tie-Line Control only**, where ACE is calculated by setting $B_f(f_a - f_s)$ to zero.

There shall be suitable display at operator screen to monitor the following parameters:

- Status and Mode of AGC Operation for each of the Area
- Graphical trend of ACE for each area
- Total Load and Generation of the respective area
- Spinning reserve (both Up and Down reserves) and operating reserve requirement of the respective area
- Spinning reserve (both Up and Down reserves) and operating reserve availability of the respective area
- AGC despatchable margin (both Up and Down margins) of the respective area

Although, during initial operation AGC will be executed in open-loop, ACE shall be conditioned (to produce a processed ACE) such that generator control action, if it were to be implemented, may occur only as necessary to reduce the magnitude of ACE with a minimum of governor control action. The AGC algorithm shall reduce governor action due to ACE noise and still respond to fast real changes of ACE by using digitally filtered adaptive and predictive controls. For each controllable unit in the system, a dispatcher selectable unit control mode shall be provided.

Actual control of a given unit shall be a function of the AGC control mode and the individual unit control mode. The capability shall be provided for software maintenance personnel to enter e.g. gains, regulating factors, assist factors, dead band values, program execution periods, and other factors as appropriate through interactive User Interface.

Initially, the length of the AGC cycle will be large enough to enable RLDC/SLDCs dispatchers and power plant operators to implement the recommended control actions. At a later date, when AGC operates closed-loop control, the execution cycle will be reduced in accordance with the real-time control requirements. In closed-loop implementation, it shall monitor control performance.

2.4.2 AGC Measurements

All unit measurements and parameters will be on the basis of telemetered generation as defined by Employer/Owner during project implementation. The following telemetered data shall be provided to the Area Control Error computation algorithm:

(a) Tie-line power flow values
(b) Schedule generation of each Unit/Plant
(c) Actual MW generation of each unit

2.4.2.1 Dispatcher Inputs to AGC

The Despatcher data entry requirements to AGC shall comprise, but not be limited to, the following functions:

(a) Select the AGC mode of operation

(b) Choose the type of computation for ACE (tie-line bias control, frequency control only, or tie-line control only)

(c) Select generating unit control mode (this capability shall be initially disabled)

(d) Enter actual interchange for tie-line values normally not telemetered

(e) Enter generating unit limits

(f) Enter unit response rates (this capability initially may be disabled)

(g) Deactivate and activate telemetry values (both analog and status)

All dispatcher entries shall be subject to validity checking.

2.4.2.2 Generating Unit Control Modes

AGC shall recognize the following generating unit control modes:

(a) Not Available: The unit is out-of-service and is unavailable to the user.

(b) Off-Line: The unit is off-line but can be brought on-line if needed.

(c) Plant Control (Local): The unit is on-line but is directly under plant control. The desired generation for the unit is determined by the plant operator.

(d) On Control (Remote): The unit is on automatic generation control and controlled by AGC within the operating limit settings.

The unit is controlled by AGC to follow the load based on its capacity.

2.4.2.3 Generating Unit Limits

The following generating unit limits shall be recognized:

(a) Total Capability: A user-entered limit indicating the maximum output the unit can maintain.

(b) Operating High Limit: A limit indicating the highest output the unit can maintain with the equipment in service at the time.

(c) Operating Low Limit: A limit indicating the lowest output the unit can maintain with the equipment in service at the time.

(d) Low Capability: A user-entered limit indicating the minimum output that can be maintained.

(e) Response: A user-entered limit representing the maximum sustained rate-of-change-of-output for the unit.

(f) Prohibited Zones for Hydro Units: Application should have capability to maintain and handle the prohibited zones of hydro units.

A check shall be performed on limits (a) through (d) & (f) to determine that the values are consistent with one another. An alarm shall be generated whenever they are not consistent and control of the affected generating unit shall be suspended until the limits are corrected.

AGC Software uses different limits while generating the plant Set Point. AGC Set Point always remains between the maximum and minimum limits available in the software.

1) Telemetered Max: This limit is the summation of the telemetered maximum value from the power plant for each unit. This limit is ideally the summation of the DC on bar value for each unit at the gross level.
2) Telemetered Min: This limit is the summation of the telemetered minimum value from the power plant for each unit. This limit is ideally the summation of the Technical Minimum value for each unit at the gross level.
3) Regulating Max: This limit is the summation of ULSP+OFFSET for each unit. OFFSET is entered manually for each unit in the AGC software. This allows LDC to restrict DeltaP.
4) Regulating Min: This limit is the summation of ULSP-OFFSET for each unit. OFFSET is entered manually for each unit in the LDC AGC software. This allows LDC to restrict DeltaP.
5) Name plate Max: This limit is obtained by considering the gross Name Plate rating and the CB status. This limit is the maximum nameplate allowed value obtained after adding the name plate ratings of all the on-bar units of the plant.
6) Name plate Min: This limit is obtained by considering the 55% of the gross Name Plate rating and the CB status. This limit is the minimum allowed value

obtained after adding the 55% of the name plate ratings of all the on-bar units of the plant.

7) Dispatch Entered Max: This limit is manually entered maximum limit for the total plant (and unit wise for hydro). Depending on requests from power plants (particularly hydro), this limit may be used.
8) Dispatch Entered Min: This limit is manually entered minimum limit for the total plant (and unit wise for hydro). Depending on requests from power plants (particularly hydro), this limit may be used.
9) In-effect Regulating Max: In-effect Regulating Max is the lowest value amongst all the limits. In-effect Regulating Max = min (Telemetered Max, Regulating Max, Name plate Max, Dispatch Entered Max).
10) In-effect Regulating Min: In-effect Regulating Min is the highest value amongst all the limits.
    In-effect Regulating Min = max (Telemetered Min, Regulating Min, Nameplate Min, Dispatch Entered Min)

The CB status and Local/Remote status may be considered for the above limits, wherever required.

<u>Additional limits and Prohibited Zones for Hydro Power Plants</u>

<u>1. P1 Limits:</u> P1 is the minimum value for the hydro power plant.

<u>2. P2 & P3 Limits:</u> P2 – P3 is the forbidden zone / cavitation zone for all the Francis turbine based hydro power plants
<u>3. P4 Limits:</u> P4 is the Maximum value (for hydro this value can be the overload value).
P1, P2, P3 & P4 are telemetered. AGC Set Point crosses the prohibited zone with the defined ramp rate.

4. Zone Count Limit is the waiting time of the AGC software for deciding whether to enter the prohibited zone, based on ACE, direction of ACE, and Actual MW. Presently this time is 5 cycles = 20 seconds. This allows AGC software to respond only for sustained ACE changes and not for momentary changes.

5. Cycle Time is the minimum time in seconds for which the AGC software waits before crossing the forbidden zone for the second time, after having crossed the zone earlier. Presently this time is set as 300 seconds. This feature will avoid frequent travel through the vibration zone for the plant. It shall be noted that there shall be a configurable threshold MW limit on Actual MW, before resetting the counter for the cycle time, if the Actual MW is in forbidden zone.

6. Declared Energy for the day in million units (MU)

7. Schedule Energy in MU (Cumulative for the day)

8. Water gross head (m)

Additional inputs for Gas power plants

1. Reference exhaust gas temperature

2. Actual exhaust gas temperature

Additional inputs for Battery Energy Storage System (BESS)

1. Minimum State of Charge SOC % permissible: It is the minimum value of SOC % up to which a BESS can be discharged. Default value would be 10-20%.

2. Scheduled Cycle (0-100%) count per day: It is the number of round-trip cycles of BESS allowed per day. Default value would be 2-3 cycles/day.

2.4.2.4 Turbine Control Logic

The desired generation for each generating unit shall be computed using the unit's base generation, the change in total generation since the last execution of the function, the unit's regulating participation factor, and PACE as follows:

UDG = UBG + - (URPF * PACE)

where:

UDG	=	Unit's Desired Generation
UBG	=	Unit's Base Generation
URPF	=	Unit's Regulating Participation Factor
PACE	=	Processed Area Control Error.

Regulating participation factors shall normally be calculated in proportion to the generating units' respective response rates. The user shall be able to enter a response rate for the calculation of each unit's regulating participation factor, but the manually entered values shall not be used for other functions requiring response rates (such as Reserve Monitoring). All regulating participation factors shall be normalized based on the units in the Fixed Load with Regulation. The unit's desired generation and all of its component terms shall be displayable.

When AGC is implemented in closed-loop mode in the future, generating units shall be driven to their desired generation in a manner consistent with the control type and the unit control modes and limits. The response characteristics of each unit shall be modelled to: (1) anticipate unit response, (2) minimize the control action that has to be sent to each unit, (3) avoid overshoot, and (4) determine when a unit fails to respond. The response models shall include stored energy effects so as to allow selected units to move faster than their response rate limit for a short period. Unit dead bands and other logic shall be used to avoid issuing control signals smaller than the control resolution of units while at the same time ensuring that control errors do not accumulate.

2.4.2.5 Generating Unit Control Signals

Some generating Plants shall be controlled by a set point representing the Plant's desired generation. A set point for each unit of such plant in control shall be calculated at plant level and unit level on a case-to-case basis as desired by the Employer/Owner and based on the change sent to generating plant by AGC. The selection of set point or raise/lower control shall be made on a Plant/Unit basis by the dispatcher.

2.4.2.6 Control Suspension/Trip

If data cannot be collected from a generating plant or if a unit has not responded within a programmer-adjustable period, the plant shall be set to Off Control and an alarm generated. Excessive deviations of frequency or ACE shall cause a suspension in control output to all generating plants until frequency and ACE are normal. During AGC Suspension, AGC Suspend signal shall be communicated to the power plants for further use by plants. The limit for these deviations shall be changeable by the dispatcher. AGC shall be suspended if the measurement from any tie line (except in the Constant Frequency control mode) or the primary frequency source (except in the Constant Net Interchange control mode) has failed. If AGC suspends control for longer than a dispatcher-changeable time period, AGC shall be tripped (i.e., control output to all plants shall cease), thereby requiring manual intervention to restore control. If the failed measurement becomes valid prior to the timeout, or if the user enters a substitute value or selects a redundant source for the telemetry prior to the timeout, or if excessive values return to within limits prior to the timeout, AGC shall resume and provide appropriate messages describing these events.

In case of power plants having daily limitation on energy/cycle, or limitation on any other parameter as per case-to-case basis, AGC suspend command shall be issued whenever the actual energy/cycle in the day exceeds the daily scheduled energy/cycle limit.

The user shall be able to trip AGC at any time. When AGC is suspended or trips for any reason, all calculations including ACE shall continue to be performed. All actions that cause a suspension or trip shall be alarmed with a message identifying the reason for the action.

2.4.2.7 Schedule Start Stop Methodology for AGC

Generating units have inherent ramp for changing their generation which is necessary to be followed at all times. Abrupt interruption of AGC application may lead to sudden variation in plant set point which is an undesirable operation for power system. So, it is necessary that AGC application shall be equipped with ramp following start-stop functionality. It is expected to keep AGC in monitoring mode (In case of creation and modification of database for SCADA, FEP, ICCP and AGC etc.) after stopping AGC operation by reducing delta P to zero (0) by following ramp rates of the units. Start-stop button shall be made available for user which start reducing delta P of all units to zero (0) by following their respective ramp rates.

Similarly, to avoid manual intervention and ramp violation while taking a plant/unit under AGC Remote, a button shall be made for each plant/unit which will make AGC Setpoint equal to the plant/unit ULSP.

2.4.2.8 AGC Performance Monitor

Control performance shall be monitored against the defined Performance Criteria. These standards are based on the combination of the ACE and the frequency deviation averages over the past twelve months. The AGC software shall have a Performance Monitor function and displays the results. It shall be possible to generate periodic reports of the performance parameters. It shall be possible to generate input vs output scatter plots and Correlation numbers. configurable for Daily, Weekly, Monthly, Annual assessments. Statistics shall be maintained as required to complete the defined Performance Criteria. These statistics shall be maintained for presentation on displays and output to a printer.

All measurements of secondary control signals from the LDCs to the plant/generator and actual response of plant/generator using SCADA data. Performance of the plant/generator shall be measured by the AGC software by comparing the actual response measured against the control signals for Regulation-Up and Down sent every 4 seconds/1 min/5 min to the LDC. Daily/Weekly/Monthly/Annual report for the plants performance evaluation shall made available.

2.4.2.9 Non-telemetered interchange / generation

The operator shall be able to enter manually the non-telemetered interchange or generation values.

2.4.2.10 Specifying Area Scheduled Frequency

It shall be possible to specify the area scheduled frequency for each of the control area.

2.4.2.11 Specifying Area Frequency Bias Coefficient (Bf)

The system operator shall be able to specify whether the area frequency bias should be calculated by software or whether it should be manually entered, and to enter the frequency bias if the manual entry is selected. The area frequency bias is represented in MW/0.1Hz.

2.4.2.12 Entering Reserve Requirements

The operator shall be able to enter/specify the Spinning reserve / Operating Reserve requirement for each of the Control Area.

2.4.2.13 Entering Operating Area Response Rate Requirement

The system operator shall be able to specify/ modify the operating area response rate requirement to be used by AGC. This value defines the minimum short-term rate in both the upward and downward direction for the entire operating area.

2.4.2.14 Selecting/Modifying a Generating Station Regulating Participation Factor

The operator shall be able to select or modify the generating station relative participation during proportional regulation duty. Alternately operator shall be able to define priority list for assigning the regulation requirement. The operator shall have the option to enter the PLC's Generators regulation participation factor (RPF) or use an RPF computed by the AGC function as per user requirement or list of priorities.

AGC shall calculate regulation participation factors for those Generators that are not using manually entered values. The manually entered values for the Generator that can regulate are added up and subtracted from 100. The amount left over is divided up among the remaining Generators that can regulate, using calculated factors in proportion to the Generators nominal up response rates. The resulting values are normalized over the set of Generators that are actually regulating (within each regulation priority) for that given cycle, to come up with the final participation factors used for the cycle.

2.4.2.15 Specify Jointly Owned Unit Operation

It shall be possible to specify some generating station for jointly owned unit operation (e.g.; SASAN UMPP which has shares in more than one control area). In such cases the generating unit shall participate for regulation for all the control area owns the generating station.

2.4.2.16 Interfacing with the Scheduling Software at RLDC/SLDCs

AGC software at RLDC/SLDCs shall design a suitable interface with Scheduling Software in line with section 8.0 web design at RLDC/SLDCs to extract the following inputs at a configurable periodicity initially set for 15-minute time block period:

- Declared Capacity of the Generating station (DC)
- Ramp Up / Ramp Down Rate
- Base Point Generation (Schedule Generation)
- Variable Cost
- Technical minimum for the plant/unit and any other value/signal as needed.

2.4.3 Real-Time Dispatch

The RLDC/SLDCs shall calculate the generation requirements for the participating ISGS based on ACE/PACE. AGC for real-time dispatch shall be performed at an adjustable periodicity. **The AGC system hardware and inputs from SCADA (viz., frequency and tie-line flows) shall be designed with redundancy in such a way that database development of SCADA and EMS Network models (transmission lines, buses, generators, etc.,) shall not hamper the real-time dispatch activity of AGC for reboots/restarts/builds etc**

a) On demand by the user.
b) Dispatcher request

c) Every Quarter of an hour/ Every Time block.
d) Change in Transmission line by tie-line bias control

2.4.4 Reserve Monitoring

The Reserve Monitoring (RM) function shall account for available generation capacity and system reserves both control area-wise and by individual generating Plant/unit. Its sizing and data interfaces shall be coordinated with OM and Interchange Scheduling & RLDC/SLDCs scheduling.

This function shall obtain input data, perform necessary calculations, and produce the results for each Plant/ generator. Reserve Monitoring shall compute the following:

- **Plant/Generating capacity:** The maximum MW output that can be committed within present operating constraints associated with the unit. This number can be manually entered by the dispatcher.
- **Spinning reserve**: The total on-line synchronized generation reserve (Up and Down).

The ability shall exist for this function to be executed periodically (user-adjustable), on-demand, and by event trigger, e.g., each time an unscheduled unit tripping takes place.

2.4.4.1 Reserve Monitoring Inputs

The input data required by the Reserve Monitoring function shall be obtained automatically, from SCADA, or manually entered by the dispatcher. The input data shall include:

- Current MW output of each generating unit
- Maximum instantaneous MW available on each generating unit
- Parameter data, e.g., rated MW capacity for each unit, Nominal reserve, MW rate-of-change for each unit.
- Forecasted Region-wise load and scheduled interchanges with neighbouring area for the next time period.

2.4.4.2 Reserve Monitoring Outputs

The outputs shall consist of the calculated values of capacity and spinning reserves both for each plant and for the entire Area. The various reserve values shall be presented to the operator on User Interface displays.

Up Reserves -

$$Up\_Reserve = Min\ of\{(In\_effect\_Regulating\_limit_{\ High} - Actual_{Plant/Unit}), Ramp\_Rate\}$$

Down Reserves -

$$Down\_Reserve = Min\ of\{(Actual_{Plant/Unit} - In\_effect\_Regulating\_limit_{\ Low}), Ramp\_Rate\}$$

i. With CB Status only
ii. With both CB Status and Local/Remote Status

Cold Reserve:

$$Cold\_Reserve = Installed\_Capacity_{without\_CB} - Installed\_Capacity_{with\_CB}$$

Margin Despatched:

Up Margin Available:

$$\left(In_{effect_{Regulating_{limit\ High}}} - AGC\ Setpoint\right)$$

Down Margin Available:

$$\left(AGC\ Setpoint - In_{effect_{Regulating_{limit\ low}}}\right)$$

i. With CB status and Local/Remote status

2.4.4.3 Reserve Monitoring Alarms

Alarms shall be generated when the following system conditions exist:

(a) Spinning reserve less than the nominal reserve

(b) Capacity for the next time period insufficient to meet forecasted load and scheduled interchange as calculated in the middle of time period.

2.4.5 Production Statistics

Production Statistics (PS) shall be provided at the RLDC/SLDCs to maintain an accurate accounting of relevant production performance, production cost, plant availability factor, scheduled vs actual generation, and daily/weekly/ monthly/annually generation regulation participation. Results shall be saved for display and trending and historical purposes and for daily and monthly reports. The following results shall be available at the end of the hour on a plant/unit and regional/state basis:

(a) Actual generation in net MWh

(b) Actual and schedule generation

For the purpose of production performance, percentage performance of the plant/unit in the day shall be available at the end of the day on a plant/unit basis.

For AGC there is need for weekly MWH account preparation for the plant/generator and for system. 3 sets of data will be used at LDC as-

a) Sent MWh AGC (convert MW data to MWh)
b) Received (MW telemetered from plant) MWh AGC
c) MWh received from plant/generators in form of .xlsx/.csv files

Provision shall be provided to compare the above data a, b & c in the plot consist of from date - To date (user selectable), with auto-scale. (5-minute data plot and 15-minute data plot. User shall be able to generate output .csv files based on the above-mentioned data a, b & c.

Generation of CSV files in user defined formats for each power plant for sending to RLDCs/SLDCs / RPCs. Before generating CSV files, subtract auxiliary consumption (in %) value from respective plant data.

2.5 Dynamic Security Assessment (DSA)

It shall be a suite of power system analysis tools that provides the capabilities for a complete assessment of system security, including all forms of stability. The software tool shall have good modelling capabilities and advanced computational methods.

The key components envisaged in the DSA suite are listed below.

- Voltage Stability Assessment Tool,
- Transient Stability Assessment Tool, and
- Small Signal Analysis Tool

The above-mentioned tools i.e., VSA, TSA and SSA shall be deployed as an on-line dynamic security assessment (DSA) tool with the SCADA/EMS System **and offline dynamic security assessment (DSA) with standard static and dynamic network models (as indicated in Table 2.1)**. In this mode, the software shall be connected directly to the Energy Management System (EMS) and assesses the system security in continuous cycles. The on-line DSA system shall provide at least the information about system security limits, critical contingencies, and remedial actions needed to prevent system failures. Also, DSA solution shall be multi user and support redundancy.

The various components of the proposed DSA Tool are described in sub-sections below.

2.5.1 Voltage Security Assessment Tool

VSA shall compute transfer limits and perform voltage security assessments using static analysis methods in accordance with voltage security criteria and contingencies. It shall contain a modal analysis tool to give useful details about the location of instability and the involvement of buses in particular modes of instability. Its remedial action module is responsible for determining the most effective procedures for preventing and correcting security violations. All analyses must have access to a comprehensive model library that takes into account crucial aspects for voltage stability, such as generator reactive capacities, switchable shunts, automatic transformer tap changers, special protective systems, and so on.

The VSA shall determine the security of the current system state (as determined by the EMS state estimator) and estimate future states (such as hour-ahead or day-ahead) for a large number of contingencies in the on-line application mode. Furthermore, much like in off-line mode, it must compute the thermal and voltage security limits of each given number of power transfers. These constraints, along with transient and small-signal security limits, will determine the Total Transfer Capability (TTC) of the system's flow-gates.

Contingency Screening: The VSA shall employ a power flow-based contingency screening method to choose a number of critical contingencies from the full list of defined-contingencies in order to decrease the number of contingencies to be thoroughly evaluated.

Scenario Definition: In VSA it shall be provided to specify a large number of scenarios to be analysed, each defined by the following:

- Base case condition (power flow)
- Power transfer definition
- Contingencies
- Security criteria
- Analysis and solution control options
- Other applicable models

VSA shall establish the voltage security limit of the transfer in scenarios involving a power transfer. VSA must decide if the base case (including contingency case) is voltage secure or insecure in the absence of a transfer definition. In either instance, a variety of reports must be generated to show discovered security violations, PV curves, voltages, flows, critical modes, and other system information.

Security Assessment and Transfer Limit: The VSA shall determine and express the security limit of any number of specified one-dimensional transfers (one source and one sink) and two-dimensional transfers (three sources/sinks). Any combination of load and generation groups may be characterised as a source or sink. Each group's generation must include a feature that can be scaled or rescheduled based on the user-defined order or share. There will be possibilities for scaling generation to meet different dispatch requirements. The security of the system and the transfer limits shall be based on the user-defined security criteria, which shall include:

- Thermal limits/Voltage stability margin
- Voltage decline/rise limits
- Reactive reserve margins

- Other criteria

VSA shall display the transfer limit and identify the restricting situation, as well as the criteria violated under that scenario.

Modelling and Monitoring: The VSA shall offer advanced modelling capabilities required for voltage stability analysis as mentioned below –

- Generator (including RE & BESS) reactive power capability (D curves).
- Various load models.
- ULTC control modes for pre-contingency and post-contingency.
- Special protection scheme (SPS) models (refer ***Appendix – B*****(B17)**)
- Combined cycle plant models.
- Flexible definition for contingencies.

The network can be modelled in the conventional bus/branch format, superimposed with optional node/breaker details for breaker-based switching actions in contingencies and SPS.

In addition, different quantities shall be monitored while performing PV analysis:

- Bus voltages.
- Circuit interface flows.
- MW and/or MVAR in groups of generators.

Solution Options: The VSA engine shall employ a specific power flow solver (Continuation power flow (CPF)) intended to deal with big complicated systems and a large number of contingencies. While obtaining high computational performance, the VSA engine must also be configured to respect numerous solution alternatives such as switched shunt controls, ULTC controls, AGC, area interchange controls, FACTS controls, and so on. It must have a specific power factor for load changes as well as a user-configurable maximum power transfer beyond which the solution will halt. Despatch must include both generating and subsystem load.

VQ Curves: The VQ curves shall be computed at user-specified buses, for all selected or no contingencies, and at any points along the PV curve. The VQ margins shall then be reported in the output analysis module.

Remedial Actions: When VSA indicates that an operating point is insecure, or the voltage stability margin is insufficient, the remedial action (RA) module shall be called to determine the most effective controls to remove all or selected security violations, or to increase the voltage stability margin to a desired value. It shall have a built-in module with following salient features –

- Compute preventive, and if necessary, corrective actions required to achieve the objectives.

- Preventive actions shall include generator voltage adjustments, SVC/switchable shunt voltage scheduling, capacitor/reactor switching, ULTC tap adjustments, and generator redispatches; corrective actions include load shedding.
- Actions to be selected based on sensitivities and their user-defined priorities.

Output analysis: An output analysis module shall be provided as a tool for managing, viewing, and plotting the results of VSA. The results shall be able to demonstrate the plot up to convergence point irrespective of even if same is achieved beyond knee point. It shall display all reports and outputs for each analysis scenario. The monitored variables (PV curves, QV curves, Interface flows, MVAR reserves, etc.) shall be plotted in various combinations. 1-dimensonal and 2-dimensional transfer limit plots shall be created for all monitored quantities. Output plots shall also be created in batch mode using scripts.

Other features: Some of the other features required in the Voltage Stability Assessment Tool are listed below.

- Feature to get integrated with EMS for real-time dynamic security assessment.
- Power system components to be identified using bus numbers, bus names, or equipment names.
- Connection with Power Flow and Short Circuit Analysis (PSA) for viewing and editing base power flow data.
- Power flow case at any point on a P-V curve can be saved.
- Contingency script utility to automatically create single and multiple contingencies.
- Data conversion tool to import power flow data in third-party formats including PSS/E, PSLF, Power Factory etc.
- Case archive feature to store or share study cases.
- Analysis of power systems of up to 100,000 buses.

2.5.2 Transient Security Assessment Tool

The TSA will be built on a non-linear time-domain simulation engine that will provide accurate response to many types of disturbances in huge interconnected power networks. A collection of security assessment modules built on this simulation engine shall perform complete evaluation for the system dynamic performance assessed by NERC or analogous system planning and operation criteria.

To meet the needs for the most demanding system studies, TSA must be setup in both on-line and study modes, with rapid calculation speed, advanced modelling capabilities, a large collection of analysis functions, and an easy-to-use interface.

Applications: The Transient Security Assessment Tool (TSA) shall provide analysis functions and modelling capabilities for the following applications –

- Transient stability analysis (rotor angle stability) for large power grids with compliancy to international standards
- Transfer limit determination
- On-line transient security assessment
- IPP integration studies
- Analysis of renewable energy sources including BESS, electrolysers
- Cascading outage analysis
- Control design and tuning (with SSA)
- Small signal stability studies (with SSA)
- Voltage stability studies (with VSA)
- Frequency stability analysis
- Design of special protection systems (SPS)
- Verification of device model and performance
- System restoration and black-start analysis
- Construction of system responses in post-mortem incident analysis
- Generation of simulated PMU signals
- Others

Exchange of Dynamic Models:

The system must be able to import the parameters of the dynamic model from the text file of standard formats (. dyr,. dyd etc.). The import process must work automatically and log all changes. The user must be able to revert the last changes. Additionally, to the automatic dynamic model import process, the user must be able to do changes to the dynamic model parameters manually.

Security Assessment: It shall consist of following as a minimum -

- **Transient stability -** a transient stability index shall be provided with a choice of computation algorithms.
- **Damping:** the minimum damping of the dominant rotor angle oscillation in the system shall be computed.
- **Transient voltage:** violations shall be captured with custom under-voltage and over-voltage criteria.
- **Transient Frequency:** violations shall be identified for a specified lower/upper range and rate of change limit.
- **Relay margin:** margins to relay operation on all monitored lines shall be computed.

- Application of security criteria shall be customizable for different regions of the system and contingencies.
- Alternative numerical integration methods shall be made available.
- All contingencies shall be ranked using any of the indices for scanning of large number of contingencies.

Detailed Contingency Analysis: Fully customized contingencies shall be easily created with the user interface provided.

- For compliance studies (such as IEGC), contingencies shall be created by pre-set rules.
- Simulations shall be early terminated to achieve fast computation speed.
- A feature for simulation of wide selection of events shall be provided as mentioned below –
  - Faults of various types (three phase, single phase, two-phase-to-ground) at bus or on a branch with auto-recloser options.
  - Branch (single, two, or three phase) tripping and/or reconnection, shunt switching, adding or modifying branch
  - Generator tripping, exciter or governor reference setpoint changes
  - Load shedding, load ramping, motor starting
  - Breaker-based switching operations
  - Pre-simulation outages and power flow dispatches
  - Dependent contingencies

Management and validation of remedial action/measures:

The user shall be able to enter possible remedial actions similarly as the lists of contingencies. For each remedial action it must be possible to associate it to a contingency or to a certain simulation result or both. For example, if the DSA solution finds out that a contingency/fault will lead to voltage instability in south, then the remedial action named "ABC" will be automatically simulated and verified as successful by the solution.

Remedial actions could be but are not limited to the following:

- Generation redispatch
- Automatic load shedding schemes
- Special protection schemes
- Wide Area Protection and Control Schemes (WAMPAC)
- Adapted relay settings
- HVDC set point change
- Any preventive load flow changes

- Topology changes

Determination of Stability Limits: The TSA shall determine stability limits in a system as per the following –

- Flexible power transfer definition (one- or two-dimension), based on the source-sink concept.
- Assessment of critical clearing time (CCT), distance to instability (margin).
- Different stability limit search strategies, including manual, binary, and fully automatic.
- Forward and backward limit searches.
- Built-in power flow dispatcher and solver.
- Determination of the maximum transfer capability on an interface, based on any or a combination of all available security criteria.
- Limit determination philosophy consistent with the similar functions in VSAT and SSA; thus, results should be comparable.

Model Library: TSA shall support and provide network and data in the node/breaker format. The TSA shall support a comprehensive model library (given below in **Table 2.1**), including the following conventional models –

- **Generator:** from classical to two-axis 6^{th} order models having quadratic & exponential saturation modelling capabilities.
- **Excitation system:** all IEEE standard exciter/AVR and PSS models and common extended models.
- **Speed governing system:** all IEEE standard models and common extended models.
- **Relay:** under-voltage/frequency load shedding, switchable shunts, distance relay, df/dt relay.
- **Load:** ZIP model, voltage/frequency dependent model, induction motor, and composite load model.
- **Renewable generation models:** Solar, Wind (Type2,3,4), Battery Energy Storage System and its various controls.

Among the advanced modelling capabilities, the TSA shall support and provide the following –

- **User-defined modelling:** function block and connectivity-based UDM approach with capability to interface with user-written control blocks. Facility shall also be provided to configure vendor specific generic model.
- **Renewable energy source models:** Wind turbines (Type 1 to type-4), photovoltaic plants, storage devices, etc.

- **FACTS model library:** SVC/SVS, TCBR, STATCOM, TCSC, SSSC, TCMCT, TCPST.
- **HVDC model library:** Two- and multi-terminal HVDC models (LCC and VSC (Bipolar and symmetrical Monopole models)), DC grid modelling, Full bridge and Half bridge based MMC based VSC models.
- **Extended term simulation model library:** Over Excitation Limiter (OEL), Under Load Tap Changer (ULTC). Special Protection System (SPS) models.

Analysis Results Monitoring: A wide selection of system quantities shall be monitored during simulations, including the following –

- **Generator:** angle, speed, voltage, mechanical and electrical power, field & terminal voltage, etc.
- **Bus:** voltage, angle, frequency.
- **Branch:** power, current, apparent impedance.
- **Load:** power, voltage.
- **Other:** generator state variables, motor/FACTS/HVDC state variables, UDM block outputs, branch interface quantities, regional quantities, etc.

Quantities to be monitored shall be customized, and system monitoring shall be specified using various options.

Case Setup and Output Analysis: The following features shall be provided –

- Connection to PSA for examining, modifying, and solving power flow.
- Connection to UDM Editor for creating, examining, and modifying user-defined models.
- Different levels of details for examining base case and transfer analysis results.
- Comprehensive output analysis module that creates various types of plots and output reports.
- Plotting module for extensive studies of simulations, with flexible plotting options:
  - Customizable x-t and x-y plots.
  - Batch plotting capability based on scripting language.
  - Data and graphics importing/ exporting facilities (ASCII text, MS Office, and Postscript).
  - Study tools such as relay analysis, case comparison, curve statistics, and mathematical Functions feature.

Other features: Some other features in Transient Security Assessment Tool to be provided are as follows –

- Feature to integrate with EMS for on-line dynamic security assessment.

- Generation of simulated PMU signals in IEEE C37.118 format from near real-time simulations
- Creation of the complete contingency set automatically according to NERC TPL standard.
- Feature of performing hybrid simulations with an electromagnetic transient simulation engine.
- Power system components shall be identified using bus numbers, bus names, or equipment names.
- Model and data verification tools –
  - Exciter/governor/renewable generator step response simulations.
  - No disturbance test simulation.
  - Injection of bus V magnitude/frequency curves ("playback simulations").
- Case archive feature to store or share study cases.
- Snapshot feature to pack a simulation for later continuation of the simulation.
- Data conversion tool to import power flow and contingency data in third-party formats including PSS/E, PSLF, BPA, etc.
- Distributed computation to enable simultaneous simulations of multi-contingency/scenario cases on multiple servers, or multiple CPU cores.
- Analysis of power systems of up to 100,000 buses and 15,000 generators.

Table 2.1 Indicative List of Models

S.NO.	List of Indicative Models
1.	**Generator:** GENROU (Round Rotor), GENROE, GENSAL (Salient Rotor), GENSAE
2.	**Exciter Models (IEEE Std 421.5):** i. **Dc Excitation** - DC1A, DC2A, DC3A, DC4B ii. **AC Excitation** - AC1A, AC2A, AC3A, AC4A, AC5A, AC6A, AC7B, AC8B, AC1C, AC2C, AC3C, AC4C, AC5C, AC6C, Ac7C, AC8C iii. **Static Excitation** - ST1A, ST2A, ST3A, ST4B, ST5B, ST6B, ST7B.ST1C, St2C, ST3C, St4C, ST5C, ST6C, ST7C.
3.	**Power System Stabilizer (IEEE Std 421.5):** PSS1A, PSS2B, PSS3B, PSS3C PSS4B, PSS4C.
4.	**Turbine-Governor (IEEE Task Force on Turbine-Governor Modelling technical report PES-TR1):** IEEESO, IEEEG1, IEEEG2, IEEE G3 (1981 IEEE type turbine-governor model), IEESGO (1973 IEEE standard turbine-governor model), GAST, GAST2A, **HYGOV, HYGOVDU** (WECC Models).

<table>
<tr><th>S.NO.</th><th>List of Indicative Models</th></tr>
<tr><td>5.</td><td>HVDC Model: Generic Line Commutated Converter and voltage source converter (VSC) based HVDC model.</td></tr>
<tr><td>6.</td><td>Renewable Solar (WECC Generic Models): REGCA1, REGCAU2, REGCBU1, DERA1</td></tr>
<tr><td>7.</td><td>Renewable Wind (WECC generic Models): WT1G1, WT2G1, WT3G1, WT3G2, WT4G1, WT4G2 along with their drive train, plant controller, aerodynamic, Electrical controller, pitch and torque controller models.</td></tr>
<tr><td>8.</td><td>
<table>
<tr><th>Drive Train</th><th>Pitch Control</th><th>Aerodynamics</th><th>Plant Controller</th><th>Torque Controller</th><th colspan="2">Electrical Plant</th></tr>
<tr><td>PANELU1</td><td>WT3P1</td><td>WT12A1</td><td>REPCA1</td><td>WTTQA1</td><td>REECA1</td><td>WT2E1</td></tr>
<tr><td>WT12T1</td><td>WTPTA1</td><td>WT12A1U_B</td><td>REPCTA1</td><td></td><td>REECB1</td><td>WT3E1</td></tr>
<tr><td>WT3T1</td><td></td><td>WTARA1</td><td>REAX4BU1</td><td></td><td>REECC1</td><td>WT4E1</td></tr>
<tr><td>WTDTA1</td><td></td><td></td><td>REAX3BU1</td><td></td><td>REECDU1</td><td>WT4E2</td></tr>
</table>
</td></tr>
<tr><td>9.</td><td>FACTS Model: Generic STATCOM and Static Var Compensator (SVC) model</td></tr>
<tr><td>10.</td><td>FACTS Model: Generic STATCOM SVSMO3T2, SVC Model – CHSVCT etc.</td></tr>
<tr><td>11.</td><td>Relay Models: Generic Distance relay models, Over voltage/under voltage relay models, Over/Under frequency relay models.</td></tr>
<tr><td>12.</td><td>Minimum & maximum Excitation Limiter (IEEE Std 421.5): OEL1B, OEL2C, OEL3C, OEL4C, OEL5CU1, UEL1 and UEL2C.</td></tr>
<tr><td>13.</td><td>Load Model: Generic model to represent composite and frequency dependent load.</td></tr>
<tr><td>14.</td><td>Generic Plant Control model: Generic generator models to playback voltage and frequency.</td></tr>
</table>

NOTE: List of latest indicative models mentioned above shall be treated as minimum. Most of these are presently being used in all India model.

2.5.3 Small Signal Analysis Tool

The SSA shall be based on linearized dynamic model of a power system or standard techniques to assess the small signal behaviour of the system. All the standard measurement-based techniques (Prony analysis, Fast Fourier Transform, matrix pencil etc) shall be implemented in SSA to cater to different types of applications.

The eigen-value computation algorithms may also be provided if it is an inherent part of the standard offering of the small signal analysis application.

The advanced computation features and analysis options in SSA shall be embedded in an easy–to-use interface to allow the user to create study cases and to specify computation tasks effortlessly.

The modelling and data requirements for SSA shall be compatible with those for nonlinear time-domain simulations (such as TSA).

SSA shall be used in a broad range of applications, including validation and calibration of dynamic models, verification of system oscillations, identification of characteristics for critical modes, system planning and operation studies, determination of stability limits, and control system design and tuning.

Computation Features: The computation features shall be provided in Small Signal Analysis Tool as per following –

- The computation of all modes in a system or in single-machine infinite-bus equivalents for all generators.
- Computation of the modes within a specified range of frequencies and/or damping (ideal for computation of interarea modes).
- Computation of the modes associated with specified generators (ideal for computation of local modes).
- Computation of small signal stability indices, including the entire spectrum or specific modes defined by frequency ranges or participating generators.
- Time and frequency response computation (useful for control design/tuning and model validation).

Case Setup: The case setup feature shall be provided in Small Signal Analysis Tool as per following –

- Create study cases and computation tasks.
- Full graphic interface for working with all data required.

Output Analysis: The Output Analysis Module of Small Signal Analysis tool shall examine all computation results from SSA runs as per following –

- Different views (tabular (listing of all mode shapes) or graphical such as contour plot) for the visualization of results.
- Various analysis tools (oscillatory modes, magnitude, damping and their graphs) to show trends and patterns from the raw computation results.
- Tools for identification of local/interarea modes, and for filtering specific modes from multiple computation scenarios.
- Case comparisons.
- Fully customizable plots.

- Data and graphics importing/exporting facilities (ASCII text, MS Office, and HTML).

Other Features: The other features of Small Signal Analysis Tool include following as a minimum –

- Feature to integrate with EMS for real-time dynamic security assessment.
- Power system components shall be identified using bus numbers, bus names, or equipment names.
- Multiple scenario processing capability.
- Feature to use single or double precision arithmetic, selectable at run-time.
- Case Archive feature to allow easy archiving and exchange of study cases.
- Batch processing
- Support and provide feature of using script language (such as Python, etc.) to extract and export computation results.

----End of Section 2----

Section-3

User Interface Requirement

Table of Contents

Section 3 User Interface Requirements

3.1 General Requirements

This chapter describes the User Interface requirements for the SCADA/EMS system. It is Employer's/Owner's intent that all functions of SCADA/EMS System shall have common user interface. All user interactions shall be from full-graphics displays.

The user interface requirements specified in this section are applicable for the user interface application of the SCADA/EMS system including Historian System and Web Systems.

Distinct User Interface for various Functions/Applications/Modules to be provided as per the requirement, merging of functionalities shall be avoided.

The proposed Historian system shall be a COTS (Commercial off the Shelf) product and it shall have a standard user interface which shall meet the functionality described in this section.

All of the features and functions shall be available to any user, except for certain functions for which access is deliberately restricted according to access control restrictions.

3.2 System Users

The term "User" is applied to the personnel interacting with the SCADA/EMS, DTS, DSA, Historian, NMS, ICCP, AGC & Web system. User and personnel-based logins shall be provided and logs shall be created corresponding to changes made by that user. These users shall be required to login in one or more of following user modes, which include:-

a) **Supervisor**: Personnel responsible for SCADA/EMS system administration and management such as assigning the access area to users, creating users etc.

b) **Dispatcher**: Personnel responsible for real-time power system operations including real-time study. They shall modify data, execute applications and perform supervisory control operations. They shall also be able to monitor the alarms and the related displays of the System Configuration of the system including that of NMS system.

c) **Engineer:** Personnel having access to certain SCADA/EMS system functions and database and responsible for support activities such as post fault analysis, report generation, regular backup of database. However, the Engineer shall not be able to acknowledge the alarms and perform Supervisory Control functions.

d) **Programmer:** Personnel responsible for continuing development and maintenance of the system functions, databases, displays and report formats.

e)**Viewer/Guest**: Personnel responsible for accessing displays and published reports such as Web Users and Remote users. These users are never allowed to modify information within the real time system, database, acknowledge alarms and execute system applications nor perform any supervisory control operation.

f) **DTS Trainer**: All DTS trainer related access and permissions.

g) **DTS Trainee**: All DTS trainee related access and permissions.

The Employer/Owner shall be able to assign the operation of certain functions, or features of functions, to specific user modes. Each individual user shall be assignable to any one or more user modes. It shall be possible to assign user workstations to modes of operation. The functions permitted for each mode is defined above.

User access to all functions of system shall follow a consistent set of common user access guidelines. A single sign on mechanism for defining and controlling user access to the system shall be provided which shall include identity authentication through independent as well as LDAP synchronized Identity Server. An Identity management application shall be deployed to manage and to help achieve seamless access to all applications after identity authentication of the users.

Password security shall be provided for access to the system, its operating system, its layered products, and other applications. Each password shall be validated against the corresponding user information in the database. Individual user shall be provided with a single set of username & password, for secured login to access all applications. Users shall have the ability to change their own passwords.

3.2.1 Identity Manager

A dedicated Identity and access management application shall be deployed (as per BoQ) to manage and to help achieve seamless access to all applications for authenticated users. **The system and users of remote consoles supplied under this project shall also be authenticated/ authorised through identity management application of respective SLDCs/RLDC.**

The identity management application shall integrate the cyber security applications, cyber security devices, networking devices and other third party application supplied under this project. Identity management system shall have following capabilities:-

a) The Administrator/Owner shall be able to assign the operation of certain functions, or features of functions, to specific user modes/groups.

b) The functions permitted for each mode and group shall be displayed in tabular form.

c) User access to all functions of system shall follow a consistent set of common user access guidelines.

d) A single sign on mechanism for defining and controlling user access to the system, shall be provided.

e) Password security shall be provided for access to the system, its operating system, its layered products, and other applications.

f) Each password shall be validated against the corresponding user information in the database/directory of the Identity management application.

g) Individual user shall be provided with a single set of username & password, for secured login to access all applications.

h) Users shall have the ability to change their own passwords.

i)Reset Password facility shall be with the Administrator/Supervisor.

j)Identity Manager shall manage to automatically Load and Reconcile Account Data.

k) Manage to identify and eliminate orphan, dormant and ghost accounts.

l)Able to maintain records/logs of changes related to access rights.

m)Able to maintain records/logs of access to workstations and applications by the users.

n) Able to maintain summary of separation of users those who are transferred, retired or leave the organization.

o) Identity server shall not be used for authentication of Web users.

p) An Identity management application shall be supplied and installed at the owner's facility by the contractor along with **minimum 100 number of client access licenses**.

3.3 Function and Data Access Security

After a user has successfully logged on, access to the functions, displays, reports, and database elements shall be restricted by pre-assigned operating jurisdictions. These operating area assignments shall be made when the function, display, report, or database element is defined. Any changes in privileges including defined in the above section for any user account should not require restarting of any servers. Application log should be saved for historian also.

The access security function shall compare the user's assigned operating jurisdictions against the operating jurisdictions assigned to the function, display, report, or database element each time a user attempts a console action, such as:-

a) Calling a display
b) Entering or changing display data
c) Viewing, editing, or printing a report
d) Web browsing from each operator console & remote operator consoles

Each user login and logout attempt - success or failure shall be logged in an activity log maintained on the system and also recorded as an event and posted to the event log. An alarm shall be generated after a configurable number of unsuccessful attempts to login and user account shall be blocked which can be unblocked by Supervisor only. Each user action shall be recorded in event log and identified by username. A feature shall be available to automatically log off the user of a workstation after a predefined period of inactivity to safeguard against users who may leave workstation unattended.

Supervisor shall be able to define time period (e.g., one year, one month, one week, one day etc.) for which user account shall be active/valid. Supervisor shall also be able to define time period (e.g., one year, one month, one week, one day etc.) for which user password shall be valid.

3.4 User Interface Environment

Displays should be based on object-oriented approach (for example, dragging a value from a single line display into a trend view to see its history). All the displays shall be accessed through web using any web browser.

A common User Interface shall be provided across applications. It shall provide a common look-and-feel across all system functions and environments (excluding Historian Systems) including the real time system, EMS, backup system, and DTS across Main and backup control centers.

The same user interface and displays used for real-time shall be used for study mode, DTS training, and historical playback excluding Historian System. A different background color or similar mechanism shall distinguish between these modes.

The user interface of SCADA system shall have provision of both white as well as dark background.

It shall be possible to save user specific choice and display configuration and same shall be made available to user whenever user logs in. UI shall allow each user to configure and savea preferred layout, size, and location of items and elements in windows and displays. The Geo-spatial display features shall provide full graphic world displays that a user shall be capable of panning and zooming. The world display features such as Layers, De-clutter levels (on the basis of voltage levels), vector overlays shall be supported. It shall be possible to use geo-spatial display for one of the layers for background from 'Google Earth/Bhuwan Maps/etc.,' as static snapshots (using already downloaded map tiles) and dynamic map-tiles (updating in real-time from Map Server) in the Geo-spatial displays. Geo-spatial display shall be updated on monthly or on-demand by users. Getting dynamic map tiles through map server shall be the Owner's responsibility but its corresponding integration and deployment in displays shall be the responsibility of contractor.

3.5 Dynamic Dashboards (SCADA)

A feature to create dynamic dashboards in SCADA, simply by selecting, dragging and dropping the points on a dashboard template shall be provided. The dashboard shall have displays like Speedometer, Bar chart, Pie Chart, real time trend, line graph etc. The speedometer display shall also indicate the limits of the analog values. A sample snapshot is attached in **Appendix-B**.

The minimum features and facilities required in the dynamic dashboards are listed below:

- Dashboards shall be definable by the end user without requiring the involvement of an administrator or programmer.
- Dashboards once created can be saved and recalled later just as any other display in the system and be refreshed with live data.
- Dashboards shall offer essential data customized to each area of interest for the user with various statistical parameters of the grid data.
- Executive dashboards to get a real-time view of the data using multiple, easy-to-read graphs.
- It should also be possible to have interactions between two displays in a dashboard. e.g., selection of one parameter or area in one display should display corresponding changes in other display.
- Display shall be customizable as per user requirement in respect of parameters like voltage, power, reactive power.
- Capability to build on-the-fly dashboard by combining subsets/Cut-Outs of different displays onto a dashboard area. For example, the user may want to monitor a particular problem in the network and will need information from a number of different displays to do it. The portions of displays that are dropped onto a dashboard display continue to be updated in real-time. Dashboards shall offer essential data customized to each area of interest for the user with various statistical parameters of the grid data. A sample snapshot is attached in Appendix-B (B10).

3.6 Display recording and playback

A licensed application in the main User Interface itself shall be delivered to capture any display screen continuously. The recording should enable playback in standard format such as mp4. The video-file shall get played in any standard video-player software. Video recording shall also be possible in historical reconstruction over a display.

3.7 Display Interactions

Display Interactions shall be consistent for all system functions regardless of the type of data on the display. It shall not be necessary for the user to learn more than one User Interface to operate or maintain the system.

Rapid, convenient, and reliable display requests shall be provided using the following methods. It shall be possible to select display from/ by:-

a) A menu display
b) Cursor target selection on other displays
c) Selection of an alarm or event message.
d) Entering a display name or number
e) Re-call command for previous display.
f) Selecting a point of interest (substation) from an Overview display.
g) Right click menu option on any display link to enable the user to open the display in a new window or active window.
h) Tagging on real-time display should be possible with facilities such as Call-Out on placing cursor on it.
i) **The content of user display can be seen any other user but can be deleted by only that particular user having access rights.**

3.7.1 Display Navigation

Display navigation methods shall provide a consistent approach for moving within a display(s). The use of appropriate methods for Panning with cursor positioning device as well as from scroll bars, zooming with cursor positioning device, Navigation window for rapid movement on a geo-spatial display and Rubber-band zooming shall be supported and there should not be any limitation to go to the previously opened displays.

3.7.2 Display Note Pad/Memo

A User shall be able to place and edit a note on any display. A symbol shall appear on the display indicating the presence of Note on that display. The content of the note shall be callable using a cursor target. The contents of these pages shall be editable and accessible by any console. The user shall have the ability to clear any page of this display and to type over previous messages.

Notes summary shall be available with "User Name" who has entered the note. A link to navigate the corresponding SLD shall be available in the same summary display Provision for "Group based Note-Pad/Memos" and "Global Note-Pad/Memos" shall be provided with following visibility requirements:-

- **Global Note-Pad/Memos:** shall be visible to all categories of users.
- **Group Based Note-Pad/Memos:** shall be visible only to specific user-group type (e.g. Dispatcher, Programmer, etc.).

3.7.3 Quality Code

All displays and reports containing telemetered analog values, device status and calculated values shall have a data quality indicator associated with each data field. The quality indicator shall reflect the condition of the data on the display or report. When more than one condition applies to the data, the symbol for the highest priority condition shall be displayed.

3.8 User Interaction Techniques

The user's interaction with the SCADA/EMS system for power system operations shall primarily be accomplished using a menu item selection technique. The first step in the interaction will be selection of the item to be operated upon. The user shall then be provideda menu of operations applicable to the selected item. The required operation alternatives include:-

a) Trend
b) Data entry
c) Device status entry
d) Scan inhibit/Enable

A set of parameters shall be presented appropriate to the item type and operation to be performed. For example, selecting an analog value for trending shall cause a menu of parameters, such as range and trend rate etc., to be presented. As appropriate for the data and function requested, a menu containing output destinations such as screen, printer, or file shall be presented. When the destination is selected by the user, the requested action shall begin.

The user shall be able to end the interaction sequence at any time by selecting a cancel command. A programmer-adjustable time-out cancel shall also be provided. Summary displays having a tabular format shall support standard User Interactions such as the abilityto sort the table by clicking on any column header, rearranging and resizing columns and the ability to filter the table contents using ad-hoc criteria entered by the end user.

3.8.1 User Guidance

The SCADA/EMS system shall respond to all user input actions indicating whether the action was

- accepted,
- was not accepted,
- or is pending.

For multi-step procedures, the systems shall provide feedback at each step. User guidance messages shall be English text and shall not require the use of a reference document for interpretation. Only employer approved mnemonics can be used.

3.8.2 Function Key Usage

In order to alleviate the operator from the repetitive task, such as calling a particular function, use of virtual keys on the monitor and function keys on the standard keyboard shall be provided.

User shall be able to define key-functions as per its requirements such as zoom-in, zoom-out, opening a specific display command to execute a particular user-defined function/operation, etc.,

3.8.3 Trending (SCADA Application)

Trending is a display of series of values of parameters on a time axis. Graphical trends shall be supported by the system for both real-time SCADA data and Historical data separately as per user selectable source for trending.

The minimum features to be provided as part of Trending are listed below:-

- Attributes of the trend display shall be user configurable.
- User shall be able to select real-time or historical data for trending on graphical displays and on tabular displays.
- Trend rate of real time or historical trend shall be user configurable and can be set to the SCADA data sampling rate for at least 2 hours without affecting the performance of system.
- Trend real-time and historical data on the same graphical and tabular trend displays (say previous day and current day frequency being trended on the same display).
- Trend different types of parameters (P, Q, V, I, F, etc.) with associated scales on the same display.
- Trending of at least 10 parameters on the same display shall be supported (with no limitation on nos. of such trend displays).
- Select a trend rate different than the sampling rate separately for each trended parameter.
- Objects like small window showing trend curve or any table in a selected display shall be provided.
- Tabular & trend presentation of the recent history (say for last 24 hours) with configurable sample time and duration of any data should be available on operator console. The user shall be able to select a trend rate different than the sampling rate separately for each trended parameter.
- Major and minor interval of x & y axis should be user configurable for any data or time. There shall not be any limitation of trends associated with a single display.
- Highlight or locate the minimum or maximum value of each visible trend through a simple user action.
- There should be provision of trending of scheduled, actual and forecasted data. It shall be possible to trend future values with current real-time data in same window for comparison.

• Trends such as "24-hour forecast/future Vs Real-time generation", "24-hour schedule Vs Real-time generation" and "24-hour forecast/future Vs 24-hour Schedule Vs Real-time generation" shall be provided. A sample snapshot is attached in **Appendix- B (B11 & B22)**.

• Plotting of trend data shall be from Left to Right (configurable).

• Any application (ICCP, CFE/FEP, AGC, EMS, SCADA etc.) point/field shall be available for trending in real-time.

• Trending for mathematically evaluated output using trended points/fields as inputs for mathematical expression should be possible.

• Multiple set of trends could be saved in an operating console and on calling the display, saved trends with corresponding configuration shall open.

• Trending application shall have standard regression functionalities like linear, polynomial and exponential etc.

• Provision for multiple y axis in trending shall be available.

• The trending of previous day and current day display must start from 00:00hrs for both the days. Further, the previous day trend should end at 00:00hrs of current day (i.e., complete 24hour duration of the previous day) and the current day trend should be up to the current time and dynamically continue to be updated as per last update data (i.e., up to the duration of last updated data for the operational day). In addition, where the display shall additionally include forecast trend for the current day, the forecast trend shall start at 00:00 hrs. of current day and end at 24:00 hrs. of the same day (i.e., complete 24-hour duration of the operational day). A sample snapshot is attached in **Appendix- B (B11 & B22).**

Points to be trended: **All SCADA points shall be made available for trending, by default. However, any system parameters such as communication or application statistics whose trend is required by user, need to be integrated as SCADA data and shall also be available for trending.**

Once the SCADA point is selected for trending, it shall display previous 24 hours history on call-up, both in graphical and tabular form. Trend database and historian database must be updated parallel with SCADA database.

3.8.3.1 Graphical Trending

The user shall be able to select and configure trending on Graphical displays enabling user for entry of the following parameters:-

a) Data values/ name along with its data quality should be indicated.
b) Trend header
c) Scales (unidirectional and bi-directional)
d) Zero offset
e) Trend data rate
f) Trend start time and date (historical and real-time data)
g) Total trend duration

h) Reference lines or shading axes (with default to alarm limits)
i) Colour (pen, grid-lines and background) shall be user configurable.
j) Current Value, legends of all axis (alias name and database name) etc.
k) Max./Min. value, time and point on the trend of the trended data along with Average value as its magnitude and horizontal line to be displayed in the trend window.
l) Drag-and-drop of a point into a trend window.
m) Trend point marker functionality to compare the data for different periods.

There shall be automatic movement of data down or across the screen as new values are generated/updated in database points/fields. When the number of real-time trend samples reaches the limit that can be displayed, the oldest value shall automatically be removed as the display is updated.

The magnitude of all the trended quantities at a particular time instant shall be displayed when the cursor is placed on the timescale on the trend display. Further, the user shall be able to scroll and zoom the viewed area forward and backward. Shading between each trend value and user-definable axis shall be provided.

The major and minor grid shall be user configurable e.g., on the x-axis the time format and displayed time shall not only be displayed as a multiple of "GMT + 5:30". A snapshot illustrating the requirement is shown in ***Appendix-B(B12).*** Trend colour shall be changeable based on a comparison of the trend value against associated alarm limits.

<u>X-Y Plots:</u>

It should be possible to plot analog values of one parameter with respect to analog values of another parameter as a two-dimensional scatter plot. Standard use cases are P-Q plots for generators, V-MVAR plots for generators, V1-V2 plots for transformers, etc.,

There should be a provision to put background characteristics of user defined co-ordinates in the x-y plots of the two parameters for which the x-y plot is defined by the user. The coordinates of the background characteristics shall be joined to form the boundary of the characteristics-polygon, over which the x-y plot shall be displayed. This feature should have the provision to be enabled or disabled by the user.

Facility to plot X-Y curve on any background where "X" and "Y" could be any user selected tag of real-time or Estimated data. An illustration is shown as at (figure-2 of Appendix II of Miscellaneous sample reports) ***Appendix B.***

Possibility of plotting one variable with respect to other shall be there in the system. For e.g., P-V curve, P-Q curve, etc., in the form of scatter plot having sample data (to shown with dot/point) with bold highlighted real-time data (to shown with dot/point). A sample curve for P-Q data of a generator is attached at (Appendix II of Miscellaneous sample reports) **Appendix B (B15)**.

A provision for having time gradient colors to the plotted points must be available so that the movement of operating point in the form of plot marks distinct for the past period and the current period can be visualized in the form of color gradient relative to the proximity of the sample time to current time in a 24-hour scale.

The current (last updated) plot mark and corresponding values must be displayed distinctly preferably in a different color. As soon as the data is updated by a newly arrived value the display attributes of current plot mark shall be shifted to the new value and the plot for the earlier value shall acquire the display attributes defined for past data plot. It should be possible for user to enable or disable this feature.

The user shall be able to print the trend on a user-selected printer without interfering with the continuing trending process.

Option of exporting of trend data at various sampling rate (user configurable) in MS-excel/csv/etc. shall be provided.

3.8.3.2 Tabular Trending (SCADA Application)

Tabular trending shall be a listing of the time-sequential values of parameters. The tabular trend shall present the data in a tabular form with one column for Date/time and additional columns for each of the trended parameter. It shall be possible to scroll up and down to see the rows. The sampling rate shall be individually definable for each tabular trend.

The user shall be able to print the trend on a user-selected printer without interfering with the continuing trending process.

3.8.3.3 Export of Trend Data

A utility for export of trend data with quality, to the PC based worksheet applications like MS- Excel and .csv format shall be provided on trend window application at a various sampling rates (sampling period, 1, 5 and 15 minute). Output of trend data shall be in parallel columns for multiple points. The option to launch this utility shall be available as a right click menu option from the trend display. It shall dump all the data available in the trend to a file compatible for the PC application.

Exporting of trended point in the form of raw and interval data should be user selectable. Trended data point exporting as interval data should have functionality for selection of time interval (secs/mins/hourly) on the trending application which could be selected by operator.

3.9 Alarms

Alarms are conditions that require user attention. All alarms shall be presented to the user in a consistent manner. Alarm conditions shall include, but not be limited to, the following:-

a) Telemetered or calculated value limit violations

b) SCADA/EMS application program generated alarms

c) Communication link failures.

d) SCADA/EMS system hardware or software failures.

e) Bus Outage in a sub-station

f) User Configurable logics

g) Temperature and Humidity Violation Alarms (for Server Room, Control Room and UPS Room etc.,)

The minimum features required in alarm messages system are listed below –

- Each alarm shall be subjected to a series of alarm processing functions.
- Alarm conditions shall be assigned to one or multiple alarm category and alarm priority levels.
- Sort, display and print user-selected alarm messages from any console by the user.
- Alarms shall also be subjected to advanced alarm processing. The results of the alarm processing shall determine the console(s) that will receive and be authorized to respond to the alarm and the associated actions with the alarm.
- There should be provision to configure alarm on real time basis for critical events like frequency drop etc. as per user requirement.
- All alarm messages shall be recorded and archived in chronological order.
- All alarms and events shall be reported to the user with reference to Indian Standard Time only. If any processing is required to make all the time in IST from the field devices, it shall be taken care by the system while doing data processing.
- Minimum 1,00,000 (One Lakhs) alarm messages shall be available in real-time.
- It shall be possible to sort, display and print user selected alarm messages from any console by the user.
- There should be provision to automatically/manually generate and sent email and SMS to the configured operator details for user defined alarms/conditions as well as selected alarms/conditions. SMS provision can be defined for but not limited to following conditions to predefined numbers: (This feature shall not be deployed globally on all parameters but shall be enabled for each type of alarms).

- Analog values crossing any of the lower or higher limits
- Change in breaker status
- Change in server status
- Change in RTU status
- Change in ICCP link status
- Change in AGC parameter status
- Change in DSA attribute status

There shall be no limitation on number of the points to be configured for this facility.

The feature of configuring conditions for sending email and SMS shall be based on user requirement for example, Outage of any critical services of SCADA system, analog values crossing any lower or higher limits, change in SERVER/RTU/device/ICCP link, change in AGC parameter status etc.

It shall be possible to configure different set of mobile numbers based on the area of responsibility defined in the SCADA system.

3.9.1 Alarm Categories

An alarm category provides the logical interface that connects an alarm condition to a specific Area of Responsibility (AOR) as defined and accordingly alarm shall be reported to user. Every alarm shall be assignable to a category. Each category shall, in turn, be assignable to one or more consoles. A means shall be provided for changing operating shifts without reassignment of alarm categories at a console. Console failure shall result in automatic reassignment of alarms to other consoles in a pre-defined manner and shall generate an alarm. Each log-on and log-off shall be reported as an event. One of the alarm category should be user configurable in real time.

3.9.2 Alarm Priority levels

Each alarm shall be assigned to an alarm priority level. Minimum 16 alarm priority levels shall be supported. Each alarm priority level shall be presented in separate display. Provision for element wise alarm for on-line Database editing shall be there.

For each alarm, it shall be possible for the programmer to independently configure the following actions:-

- Audible alarm tone type selection and its enabling/disabling. Minimum 5 alarm tone shall be supported by system. The silencing of audible alarms shall be recorded as event.
- Alarm messages to be displayed on an alarm summary.
- Alarm message deleted from alarm summary when acknowledged.

- Alarm message deleted from alarm summary when return-to-normal alarm occurs.
- Alarm message deleted from alarm summary when return-to-normal alarm is acknowledged.
- Alarm message deleted by user action.
- Alarms message shall be generated in SCADA system for events such as failure of primary source of data.
- User shall be able to define individual point for audible sound, SMS, Email alert.
- Every Alarm shall be accompanied by an Audible tone (different audio tones for different types of Alarms configurable by the user) which shall be user configurable also in real time for some particular events also, like:-
    - Frequency drop,
    - Overloading of some important lines,
    - Generation tripping of important stations (individual and total),
    - And aas per the operator's requirement etc.

Customized audio alarm for example, tripping of 765/400 KV lines and other critical elements. A dedicated display shall be provided for selection of Audible Tone in separate category of Alarms. The automatic generation and sending of an E-mail and SMS containing operator selected Alarm or user-defined data shall also be possible. Alert function shall be provided which shall allow notifications to a single or a group of operators.

This assignment shall determine how the alarm will be presented, acknowledged, deleted, and recorded. All acknowledged Alarms shall be reported as an event along with the identification of user and/or the workstation.

3.9.3 Alarm Management

Additional standard products for advanced alarm management shall be provided. Minimum features of the alarm management function, as available in the standard product shall be supplied which may include:-

(a) Minimization of nuisance alarm messages (e.g., repetitive alarms for the same alarm condition)

(b) Highlighting of the most urgent messages

(c) Display of Alarms Substation wise

(d) Sort, filter of alarms by users by node, element, type, date & time

(e) Suppression of chattering alarms: The chattering of alarms shall be prevented from occurring in the system. In case a switching device's state is changed from OPEN-CLOSE (or vice-versa) more than a user-defined number of times within a user-defined time-interval, then it should be blocked from getting listed in Alarm list with set/reset of a dedicated flag and corresponding alert shall be issued to the operator for this action.

f) Alarms related to device state may be required. For example, following may be considered:-

- Voltage magnitude based Reactor in/out status alarm. If V>threshold => BR should be switched in.
- Reactive Power management as per capability curve of generator and prevailing voltage of selected buses.
- Alarms related to device state may be required. For example, following may be considered.
- Voltage magnitude based Reactor in/out status alarm. If V>threshold => BR should be switched in.
- Reactive Power management as per capability curve of generator and prevailing voltage of selected buses.
- Alarm based contour & heatmap on network map. For e.g., if there are large no. of alarms, it would be useful to see where the major alarms are concentrated or originating from.
- Lines which are out / not in service.
- List of Open-ended lines.
- List of lines/transformers where loading is more than desired limit (say 80% of alarm limit) etc.
- The line should flicker in the display, when tripped.

Alarms shall also be subjected to advanced alarm processing. The results of the alarm processing shall determine the console(s) that will receive and be authorized to respond to the alarm and the associated actions with the alarm.

3.9.4 User Interaction for Alarms

The User shall be able to perform the alarm interactions described below:-

- Alarm Inhibit/Enable

- Alarm Acknowledgment
- Change Alarm Limits
- Annotate an alarm by adding a comment
- Copy / Paste Alarms into a spreadsheet and all MS-Office formats for offline analysis.
- Alerts: Alert function shall be provided which shall allow notifications to a single recipient, a group of contacts, or an entire escalation team that reflects the organization's chain of command whenever operational excursions occur. These alerts shall be sent through email for remote users. The Alert shall have the ability to interface with SMTP server for emails etc. Alerts shall be user-definable based on any configuration logic.

3.9.5 Alarm Presentation

Alarm presentation shall be determined by the alarm's category and priority. Displays shall highlight every alarm condition using a combination of colour, intensity, inverse video, and blinking. In addition to display, audio annunciation for user-selected categories alarms (as discussed in earlier section shall also be provided.

The alarm condition highlighting shall show whether the alarm has been acknowledged. The highlighted alarm condition shall appear on all displays containing that device or value at all consoles regardless of the alarm'scategory.

Provision for global alarm setting (operational, alarm and emergency limit) shall be provided.

Alarm messages shall be a single line of text describing the alarm that has occurred and the time of occurrence. The alarm message shall not require the use of a reference documentfor interpretation. The alarm message shall be easily interpretable with its colour, intensity and blinking feature etc.,

The user shall be able to change the alarm limits (operational, alarm, emergency, reasonable etc.), inhibit/ enable alarms and acknowledge alarms. All actions (except acknowledgments) shall be logged as events.

3.9.6 Alarm Window

Each screen shall include a scalable window containing symbols for substations, generating stations, computer system facilities and others. These symbols shall blink when an alarm condition is detected for a device or value associated with the symbol. Blinking shall cease and the symbol shall be highlighted when all alarms associated with the symbol are acknowledged.

The symbol shall return to its normal presentation when the last alarmassociated with the symbol is deleted. Cursor selection of the symbol in alarm shall result in the presentation of a display associated with the symbol.

A special alarm window shall be provided, in which the most recent alarm messages shallbe displayed. All alarm summary views shall support ad-hoc sorting. Clicking on a column header in the alarm view (time, station, Element/Equip, Region, State and priority, etc.,) shall sort the alarms by that column.

All summary alarm views shall support ad-hoc filtering in which a user can specify filtering criteria in order to easily locate specific types of alarms. Examples include, but are not limited to:-

a) Specific Time/Date ranges
b) Alarms exceeding a particular severity
c) Alarm messages containing particular device names
d) Alarm messages containing user annotations
e) Filtering on basis of device type, line name, etc.

It shall be possible to save any number of filtered alarm views for easy retrieval in the future.

3.9.7 Alarm Help

A context-sensitive help facility shall be included in the SCADA/EMS. When an alarm matching a predefined type is generated, the alarm presentation should include an indication that additional help is available. Clicking the alarm help indicator shall invoke an alarm- specific help screen that contains specific help information (user configurable) for that alarm. The contents of the help screen shall be defined by the administrator.

3.9.8 Events

Events are conditions or actions that shall be recorded by the SCADA/EMS system but do not require user action. Events shall be generated under the following conditions:-

a) User initiated actions
b) Conditions detected by application functions that do not require immediate user notification, but should be recorded
c) Values returning to normal from a limit violation state.

Events shall be recorded in the form of an event message. The event message format shall be similar to the alarm message format. Event messages shall be displayed on an events summary.

Event messages shall be archived in chronological order. Minimum 100000 (One Lakhs) event messages shall be available in real-time. It shall be possible to sort, display, filter and print event messages from any console. The feature to extract event messages in MS-Excel, CSV, etc. shall be provided.

3.10 Hardcopy Printout

The SCADA/EMS system shall have features to produce a print out of a display, reports, trends, alarms, events, etc. from a menu. It shall be possible to take print with various options e.g., Print the viewport, Print the complete display adjusting to a specified page size, Print a selected portion of a display or screen.

The displays shall be printed with white background by default. The borders of the viewport, rulers, file tab shall not be visible in the printout of any display unless specifically chosen. Multiple page displays shall have page numbers like Page X of Y. Also, the options for printing shall include at least choice for orientation, background colour, page size, colour/ black & white and print preview.

All hardcopy printout shall include the following additional information apart from the display print out:-

a) Date and time of the print out
b) Name of the user who has given the print out command
c) Identification of the console from where print out was generated
d) Name/ Identification of the display
e) Entire Display (Geo Map, SLDs, Summary Displays etc.) should be able to print selectable printer and in the form of PDF. Display resolution could be auto-adjustable to fit the entire display for PDF creation with clear visibility of all parameters.
f) Entire Display could be print for any mode of display (historical/playback value, estimated values, OTS mode).

Snapshot of any display full and part there of if required should be printable in a fit to page format. The printout of the display, reports, etc. shall also be made available in PDF-format along with corresponding licensed software.

In case of printing of large geographical / map / SLDs display into a pdf format, the complete (not limited to the visible portion) display (Map) shall be converted into pdf file format with high resolution so that the values/texts plotted in Maps in pdf format shall be clearly visible and readable after zooming the pdf file. If any additional software is required, the same shall be provided by the contractor.

3.11 Dynamic Data Presentation

It shall be possible to present any item in the database on any display. All data control capabilities shall be supported from any window of a geo-spatial, SLDs, and other displays. Device status or data values shall be displayable anywhere on the screen, excluding dedicated screen areas such as the display heading.

All fonts supported by the operating system delivered shall be supported by SCADA/EMS system. Standard X-Window system fonts shall be provided with the SCADA/EMS. Regional languages (as per local language of different states under the regional projects) and Hindi fonts (true type fonts) shall also be supported. All fonts supplied shall be supported on the user interface devices and all printers supplied with the system. The types of fonts to be used in a particular display shall be selected at display definition time. It shall be provided to change font colour & size on any display. There shall not be any limitation on the colour and size used for the fonts.

Status and data values shall be presented in the following formats as appropriate:-

a) Numerical text that presents analog values, sign and flow direction arrows.

b) Normally the telemetered MW-MVAr values along with the sign and direction shall be displayed on the Single line diagram (SLD) and Network diagram. Bus Voltage & Frequency shall also be displayed on SLD & Network diagram.

c) Symbols, including alphanumeric text strings for an item, based upon state changes e.g., circuit breaker (OPEN/CLOSE/ INVALID).

d) Symbols, including alphanumeric text strings for indicating the data quality flags.

e) Colours, textures, and blink conditions based upon state or value changes or a change of data quality, e.g., alarm limits.

f)Display of static as well as dynamic fields at any desired angles shall be possible e.g., Static Text of "MW" flow of a line aligned with the line on the geo-spatial display.

g) In case of Blackout incidence in any substation, the substation symbol should display in blinking mode. Sample Display building approved guidelines are attached at **Appendix-K,** the same shall be followed.

3.12 Element Highlighting

Element highlighting techniques shall be provided to draw the attention of Dispatcher to critical state of the system. The highlighting technique such as, change of colour, size, colour intensity, blinking, Character inversion, Line texture, appended symbols etc. shall be supported.

This feature shall be used to highlight alarms, power system device and measurement status, data quality, data entry locations on a display and error conditions. Conditional attributes effect (such as dotted line in case of opening of a line) shall also be provided in the display.

3.13 Display Types

The following list describes the type of displays that are to be included in the SCADA/EMS system. All displays shall have default setting for showing Date & Time. The energized/de-energized state of the Power System elements shall also be identified, based on SCADA topology processing, as per requirement.

3.14 SCADA/EMS System Display

A display shall be provided that lists all SCADA/EMS system directory displays. The displays shall be listed in alphabetical order with suitable separation in the list to enhance readability. Each entry in the list shall have a cursor target for display selection.

The displays shall have layered architecture with full control of individual layer, 3D movement by moving the display operator shall be able to see the limit violation in form of bar/cone/etc. in order to quickly pin-point the pain area. Display features such as Auto-fit to Screen shall be provided. Mash-up interface with standard map-service providers such as "Google Earth/Bhuwan/Open Street Map etc.," shall also be provided.

The visualization tool supplied under this project shall be a tightly integrated decision support tool with SCADA/EMS System tailored to the operational objectives of the system with advanced visualization techniques to concisely and intuitively present users with essential Energy Control Center data.

This tool shall have advanced features such as 3D visualizations, geo-spatial maps, contouring, and other objects to enhance operations and significantly enhance situational awareness in the control room.

All workstations shall be provided with the SCADA/EMS graphical user interface including the visualization tools for 3D displays, geo-spatial maps, contouring etc.

There shall not be any limitation in opening, editing of database and display from any of the workstations supplied under the contract. User shall be able to edit from any workstation after login with proper credential.

A search facility for finding the desired display from the display index/directory shall be provided. A feature to "find/search" stations in the geographical display shall be provided.

An advanced version of graphic builder shall be provided so that network diagram can be made and modified with actual geographical coordinate. The tool should be capable of adjusting the overall display automatically in such a way that it allocates space for the new addition.

3.14.1 Power System Network Display

A Graphic overview of power system network display of the lines, feeders, network elements colour coded by voltage shall be provided. This display shall present the transmission system in a graphic format as listed below.

a) Telemetered and calculated data like Real and reactive power flows shall be displayed as a value with a direction arrow.

b) Lines shall be displayed with a direction arrow with respect to direction of power flow & its value indicated on the line itself.

c) Lines that have exceeded their loading limits shall be highlighted.

d) Substations and power stations shall be depicted by symbols that reflect the presence of alarms at that substation or power station.

e) Cursor selection of a substation/ power station symbol shall result in the associated Single line diagram display for that substation/ power station.

f) Graphic overview of overall power system network display indicating the important feeders/network elements shall also be provided.

g) Provision for making selection among multiple sets of busload distribution factor, to find the BLF output shall be made available and display for BLF output shall be made available on Network Display. This Bus load distribution factor should be derived from load profiles of the modelled system.

h) Tool tip (information of the icon/field /picture to be displayed on hovering with cursor) facility to be provided show line length, conductor type. Sample display is attached in **Appendix- B(B20).**

i) Display shall be showing Active Power, Reactive Power and Estimated values with facility to search on geographical Map.

j) Display shall have facility of contour & Heatmap based on Voltage, Animations of line loading.

k) The substations mapped in the grid diagrams shall be geographically mapped so that exact geographical locations of substation can be displayed in the grid diagrams.

3.14.2 Interchange Display

The interchange display shall be provided as a schematic diagram showing power transfers between various area/ utilities/ entities. This diagram shall show each power system as a block with actual and scheduled net interchange values outside/ inside the block respectively. Symbolic arrows shall indicate power flow directions. The diagram shall also show schedule deviations. This display shall show the frequency values from substations having tie-lines.

3.14.3 Sub Station Single Line Diagram (SLD) Display Menu

A display shall be provided that lists all substations that can be viewed via a SLD. The name of the SLD displays shall be listed in alphabetical order, according to substation name, with suitable separation in the list to enhance readability. This display should be updated automatically after addition of a new substation. Each entry in the list shall have a cursor target for graphic display selection. The menu selection shall allow the user to view the SLD display menu. It should be possible to filter the substation list with area, division, highest voltage level etc.

3.14.4 Sub Station SLD Displays

SLD displays shall be provided for the monitored substations. Each display shall present telemetered, manually entered, estimated and calculated power system data on a Singleline diagram that shows substation layout in terms of its buses, switches, lines, and transformers.

The feeder names in the SLD shall have linkage with remote substation end SLD associated with that feeder. It shall be possible to move to remote-end substations SLD by selecting this feeder.

The user shall be able to perform any user interaction defined by the Specification on these displays. In the SLD the device names should be displayed along with each device. The names shouldbe automatically generated from the database at the time of creating such displays. A pop-up containing relevant details (such as real-time value, sub-station, area, important flags, option to manually replace, plot-trend, last update time etc.,) related to the switching devices and analog points in the SLD shall open with-click on the respective symbol/data.

Displays shall be "display-fit" and there should be no unutilized space. Estimated data shall also be shown on the display. The user shall be able to perform any user interaction defined by the Specification on these displays.

SLD shall have linkage to all the alarms pertaining to that substation.

3.14.5 Sub - station Tabular Displays

Tabular displays shall be provided for each substation which could be open in single click with in SLD display. These displays shall list the real-time values of telemetered (Primary, secondary and alternate sources etc.), manually entered, and calculated data associated with the substation as well as related information such as alarm limits. Each calculated data point should also display the input variables/data points within it along with quality. The user shall be able to perform any user interaction defined by the Specification on these displays. It shall also show the max/min/avg of pre-defined period i.e., 5 min./15 min./30 min./60 min./6 hr./12 hr./24 hr. data with time-stamp and these periods should be user selectable. Sorting, filtering features shall also be available in tabular displays. Option of creating customized tabular display based on user requirements shall be provided. The details of the same shall be finalized during detail engineering.

3.14.6 Other Tabular Displays: Some customized tabular displays for listing of data on special conditions shall be provided such as -

a) Bus Outage display

b) Reactors in-service/not-in-service display along with MVAR consumption.

c) Open Ended Lines display

d) Highest loaded ICTs display

e) Over loaded line display

f) HVDC system display indicating active power flow ad reactive power consumption from HVDC terminals.

g) FACTS devices VAR consumption display.

h) Series Devices bypass/open status with MVAR absorption.

3.14.7 Alarm Summary Displays

Display that list or summarize all unacknowledged and acknowledged alarms shall be provided. The summary shall separate acknowledged and unacknowledged alarms. Capacity shall be provided for alarm messages for each alarm summary type. If an alarm summary display becomes full, the oldest messages shall be automatically moved to System Message log and the newest messages shall be added. It shall be possible to perform any alarm interaction from this display.

Sorting and filtering of alarms on the basis of area, station, voltage level, device type, etc. or any of the combinations of these shall be provided.

Time of alarm received in SCADA and time stamp of field both must be available in the display.

3.14.8 Event Summary Displays

Event Summary displays shall list the most recent events and shall be organized by category for those categories assigned to a given console, as one summary display for all categories assigned to a console, or by all conditions system-wide without reference to the categories assigned to a console, as selected by the user. The user shall be able to select between viewing events in chronological or reverse chronological order.

3.14.9 Operating Information Summaries

The operating information summaries defined below shall be provided. Summary items shall be listed in reverse chronological order with the most recent item shown on the first page, timestamp of manually marked shall be available and filtering shall be possible. All summary displays, shall be information-only displays; no user interaction other than display call-up, shall be associated with them. Operating information summary shall have:-

a) Manual Override Summary

The manual override summary shall list all telemetered and calculated device status and data values for which a user has substituted a value.

b) Off-Normal Summary

The off-normal summary display shall list devices and values that are found to be abnormal, i.e, are not in their normal state. Telemetered, calculated, and manually entered status and data values shall be included.

c) Out-of-Scan Summary

The out-of-scan summary display shall list device status and data values that are not currently being processed by the system. If an entire telemetry source such as a data set is out-of-scan, the out-of-scan summary shall display the source without any of the individual device status or data values associated with the source.

d) Alarm Inhibit Summary

This display shall list devices and data values for which the user has suspended alarm processing.

e) Graphical Trending Summary Displays

The summary display shall list all items being trended. The list shall include the item name, trace number or colour, trend orientation, and trend range. Real-time visualization of data should be possible in graphs such as Pie, Scattered, Surface, Load Duration Curves, Contours, Three-dimensional, data represented in the form of Analog meters, Bar graphs, line graphs, etc.

f) Tabular Trending Summary Displays

The summary display shall list all items being recorded for tabular trends. The list shall include the item name and the file name.

g) Note Pad Summary Displays

This display shall list all the notes attached with displays.

h) Stale/Freeze Data Display

This display shall list the analog points based on SCADA UI for which the rate-of-change of value is "Zero" for a specified period (as defined by the user) of time.

i) Data Validity Display

This display shall list all the analog data for which the "Data Validity Checks" have beenviolated such as follows:-

- Line/Feeder MW comparison with other end data crossing more than a specified limit.
- Bus Voltage kV comparison with the other bus kV of same voltage level in a sub-stationmore than a specified limit.
- MW/MVAR Summation at same system voltage level in a sub-station.
- Other similar data validity cross-checks.

j) Operations Monitor Display

In the Operations Monitor Display, the following quantities as a minimum need to be displayed with EMS database and SCADA measurements. SCADA measurements calculations shall be user-definable for Actuals MW/Net interchange/Tie-Line Exchanges etc. –

a) Power system frequency from multiple sources in the area (instantaneous values and average values initially on a 5-min basis)

b) Actual Generation MW

c) Net Interchange MW (actual, scheduled, and deviation from schedule): Net Interchange definitions and calculations shall be user-definable

d) Actual Load MW (including transmission losses)

e)Transmission capacity for defined pair of nodes, corridor & axis in the system

- Currently used
- Balance Available

f) ACE (Area Control Error) within state

g) Tie Line Exchange

h) Net Load (MW), Renewable Generation (MW)

i) Spinning Reserve available (Pmax. – Pmin.)

j) Delta P incremental value, trend for all generator participating in AGC

k) AGC ON/OFF in respective software at Load Dispatch Centre as well as for particular generator/plant mode of operations Local, Remote etc.

l) District wise/city wise load profile display diagram

m) Display of Discom wise power demand

n) Statutory regulations based required calculations (eg. Zero crossing block, Deviation Settlement Mechanism etc.) should also be configurable along with alarms.

3.14.10 Computer system Configuration and Monitoring Displays

Graphic and tabular displays shall be provided that allow the user to:-

a) Monitor and revise the configuration of the computer system supplied under the project.

b) Monitor the system's resource utilization statistics.

3.14.11 Communication Network display

This display shall show information of RTU & ICCP communication display of the status of the communication links being used for data exchange with other control centres respectively in real time SCADA system. The display shall also indicate the healthiness of standby communication links. Failure of main or stand by communication links shall be suitably alarmed. Active channel should be differentiated from other channels by suitable indicators. Sample display is attached in **Appendix -B(B21)**.

Provision shall be provided to enable/disable the RTU and to view RTU details such as object address wise raw value, processed values, baud rate & all the other parameters through respective User Interface (UI). Report for percentage availability of individual/multiple communication channels shall be generated for user defined interval.

3.14.12 SCADA/EMS Application Program Displays

Application program displays shall be provided to satisfy the user interface requirements of the system functions stated throughout this Specification. Application program displays shall be based on a standard user interface design across all applications to provide a common look and feel. The application's information shall be presented in such a way as to facilitate user operations.

3.14.13 State Estimation Display

The result of state estimation shall be displayed on the following:

- Network diagram along with SCADA data.
- Geo-Spatial Map
- Tabular Display

3.14.14 Contingency Analysis Display

The result shall be displayed on the geo-spatial map and also on 3D display clearly highlighting elements violated with width of the element/ height of 3rd dimension proportional to post contingency solution value and status change, if any.

3.14.15 Transmission Corridor Displays

The user shall be able to select any two nodes from the network diagram to get the TTC, ATC, UTC Values & angle between the selected nodes as defined in EMS section. The display shall be provided in graphical and tabular manner.

3.14.16 Contour & Heat Map Displays

It shall be used for showing large amounts of spatial data e.g., bus voltage magnitudes (in p.u.), percent loading of lines (with respect to Surge Impedance Loading SIL), flow-gate values and weather data. Displays shall be with facility of appearance of visual alarm of underlying layers and background color for gradient before alarm.

Contour (**Appendix B(B7)**) & Heat Map (**Appendix B(B28)**) of following analogs shall also be available:

- Angle contour
- Line Flow contour/Heat Map, Overloaded Lines contour/Heat Map, Weather contour/Heat Map, Generation contour/Heat Map, Load contour/Heat Map, etc.
- Contour & Heat Map of Bus summation should also be available so as to help in getting the mismatches in the data.

If redundant MW and MVAR measurements are available in the station then the operator should have and dedicated station-wise display in order to select/deselect the extra analogs used in bus summation.

Geo-spatial display with contour map of Data within geographical boundary of India shall be provided in which Zoom-in, Zoom-out, Panning option shall be available in the map. Display Builder shall be capable of importing point and placing a predefined picture/symbol as per the Latitude and Longitude specified by the user.

The" Playback" option shall be made available in the map so that the continuous pattern over the period of time shall be visualized. The pattern shall be exported in a video format so as to use it in offline mode.

The displays mentioned above need to be shown on an interface with background such as Google Map, and it shall have provision for updating manually the latest background map as per user requirement during the project life cycle.

3.14.17 Voltage Profile Display

Voltage profile displays shall be provided to present different voltage levels on a geographical display in form of contours & heat map. Further, the areas with various voltage levels shall be shown with different colours.

Another voltage profile display shall be provided in form of three-dimensional (3D) display showing voltage contours in a time scale (e.g., voltage levels at Morning Peak, Day off Peak, Evening Peak and Night off Peak etc.) with different colours.

The displays mentioned above need to be shown on an interface with background such as "Google Map/ Bhuwan/ etc."

3.14.18 ICCP Database Editing Display

ICCP database modification display shall be provided to do incremental changes in ICCP database (e.g., addition/deletion of individual Status/Analogue data or a stations entire dataset for any ICCP link of that Control Centre.) using standard editing tools of full graphics windows User Interface e.g. cut, paste, copy, drag, drop etc. from the ICCP and SCADA database. Above dedicated display can also be a part of database development system. However, it should facilitate all above interaction to achieve ICCP database changes.

3.14.19 Help Displays

Help displays shall be provided to aid the user in interpreting displayed information and to guide the user through a data entry or control procedure. Help displays shall be provided for each display that is provided with the system. Each display shall have a prominent cursor target that the user can select to request the associated help display. For standard displays, software aids (such as context sensitivity) shall be used to present pertinent help information in an expeditious manner. A programmer shall be allowed to modify and create help displays.

3.14.20 Historian Data display

Historian display shall be different from other displays and shall have user friendly features through tabs and icons for events, major disturbances, outages etc. for quick report generation for a defined time period. Recently and frequently used fields for report generation and configuration shall be stored as "favorite" reports. The display shall have drop down menus for:

- Data (Elements, (MW, MVAR, Min, Average, Max, etc.) View with calendar function for selection of Year, Month, date and time.
- All the features mentioned in for historian under SCADA System Function shall be meet.

On the display, Provision for selection of format shall be made available (option for word/ Excel/PDF) with Export button. On the top of the display types of reports should be displayed, e.g., Daily report, monthly report, etc.

3.14.21 Web Server Displays

The web servers shall provide access to remote clients through commercially available Off-The-Shelf (COTS) Web browsers. External users shall be able to open web displays without downloading/installing any software etc.

The web server shall use the same SCADA/EMS displays but render it through web-servicesto the remote clients.

3.14.22 Generator Capability Curve Displays

The display shall show - PQ Generation vis-à-vis PQ capability curve in continuous shifting pattern. A sample illustration is included in (**Appendix -B (B13 and B14)**) given for the same. These displays shall be available in SCADA and historian as well.

3.14.23 Real-time data trail on operating curves/quadrant of special power system devices

The real-time data representation (along with its trail for last 24 hours) on operating-curves of devices such as STATCOM, etc. shall also be provided.

The quadrant of operation as per the real-time voltage data (along with its trail for last 24 hours) in case of transformers shall also be presented. The detailed requirement and customizations shall be discussed during detailed engineering. A sample illustration is included in (Appendix -B (B15)) given for the same. These displays shall be available in SCADA and historian as well.

3.14.24 Weather data on Geographical map display

The display shall show the weather data superimposed on a geographical display with background such as "Google Maps/Bhuwan Maps/etc." A sample illustration is included in ***Appendix –B(B16).***

3.14.25 Special Protection Schemes (SPS) displays

SCADA/EMS system should support and provide logical diagrams such as SPS, conditional operations including various parameters, etc. It includes various functions as follows:-

a) Rate of change of flow
b) Status position
c) Voltage data value
d) Direction of flow
e) Total power transfer through a corridor
f) Load shedding feeder's analog and digital data
g) Logical operator functions such as AND, NAND, OR, NOT, NAND, etc.
h) Combination of all above mentioned factors with involvement of multiple tags simultaneously.
i) Alarm shall be generated in case of SPS operation (on pre-defined conditions). The complete list of SPS displays to be made would be given at the time of detailed engineering. A sample illustration is included in ***Appendix -B (B17)***.

3.14.26 Market Applications Display

The display shall provide the information based on static text, dynamic real-time data and trending of data mentioned in Section on "Data Exchange with Market Applications and OpenAccess" of ***Part B.*** A sample illustration is included in ***Appendix -B***.

3.14.27 GUI for online editing of ICCP

GUI for On-line editing of ICCP database shall be made available to the user. Proper Graphical User Interface for online editing of the ICCP database and mapping with other control centers should be provided.

3.14.28 Telemetry Information Summary Display:

Tabular display with filtering of entire telemetered data should be possible using operators such as AND, OR, NOT or any other means and sorting should also be possible on the basis of Region, Division, Voltage level, type of equipment, data type, data quality, substation, generating station etc. in ascending, descending and alphabetical order, If operators such as AND, NOT & OR is used then it must support nesting of operators.

3.14.29 Integration with Electronic Documents

Information related to power system equipment often resides in standard format electronic documents (PDF, DOC, XLS, JPG, etc.). In order to minimize the time for users to locate this related information when needed, the user interface shall provide a mechanism for accessing electronic documents related to any device on a display. This shall be through right-click menu option or similar.

Examples of Electronic Documents that should be available in this fashion include:

- Digital Images.
- Equipment Manufacturer documentation (PDF or HTML).
- Maintenance and other Historical Reports.
- Switch Orders, etc.

………..End of Section 3…………

Section 4
System Software Requirements

Table of Contents

Section 4 System Software Requirements

4.1 General requirements

This section describes the characteristics of system software such as Operating system, and support software (compilers, database development and maintenance, display development, network services, Report generation, diagnostics, security and Backup utilities) provided by Contractor and the original equipment manufacturer (OEM) as necessary to support the applications of SCADA/EMS system. This section also describes the standards to be followed for all supplied software.

Bidder has to provide the latest version of all SCADA/EMS Application software supplied under the project before the start of Site Acceptance Test (SAT) without any cost implication.

Bidder has to provide the latest version of all third-party application software supplied under the project before the start of Factory Acceptance Test (FAT) without any cost implication.

The contractor shall provide details of all the API's including its source code supplied/used under the contract to the owner without any additional cost.

4.2 Software Standards

All software of SCADA/EMS system provided by the Contractor, including the Operating system, Database and support software, shall comply with the industry-accepted software standards. 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. The Contractor shall commit to meet the "open systems" objective promoted by industry standards groups.

4.2.1 Design and Coding Standards for SCADA/EMS applications

All applications of SCADA/EMS system shall be maintainable by owner using the supplied software utilities and documentation. The software design and coding standards of SCADA/EMS system shall address the followings: -

a) **Expansion:** Software shall be dimensioned to accommodate the size of SCADA/EMS system as given in the specification.

b) **Modularity:** Software shall be modular i.e. functionally partitioned into discrete, scalable, reusable modules consisting of isolated self-contained functional elements and designed for ease of change. The system shall make maximum use of common industry standards for interfaces.

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

d) **Conformance to SOA:** The software shall confirm to Service Oriented Architecture (SOA).

e) **Enterprise Service Bus (ESB)**: ESB based architecture is essential to enable interaction of applications from different product manufacturer, platforms, etc.,

f) **Portability & Interoperability:** The system shall be designed for hardware independence and operation in a network environment that facilitates interoperability and integration of third-party applications. SCADA/EMS shall support multiple database systems including Oracle, Microsoft SQL Server and MySQL.

g) **Programming languages:** The software shall be written using high level ISO or ANSI standard programming languages.

h) **Antivirus Software** - All computers and firewalls shall be provided with the latest antivirus software as on date of supply. The antivirus software shall have the capability of having its virus definitions updated from time to time. The Contractor shall be responsible for the maintenance & update of the antivirus software.

The system shall confirm to SOA (Service Oriented Architecture) and abort processes taking long time for executions. The programming languages used in the system shall be written using ISO or ANSI standard.

4.2.2 Operating System

The operating system of all the equipment of SCADA/EMS system including network equipment shall be latest version released preferably up to six (06) months prior to FAT.

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

The operating system shall be hardened to provide robust security. In order to facilitate cyber security requirements including patch management, common operating system is preferable to be used by all server nodes within the SCADA/EMS including real-time servers, application servers and ICCP servers.

The system security shall also be maintained in line with cyber security guidelines/ recommendations issued by statutory authorities **like CEA, CERT-In, NCIIPC etc.**

from time-to-time throughout the life cycle of the project.

Operating System and Software Upgrade:

Keeping in view the long duration of maintenance services and probable end of support for deployed Operating system or 3rd party applications, following should be done for Upgrade:

- In case of end-of-life, obsolescence and end-of-support of the operating system, Anti-Virus or any other software delivered in the project, the contractor should provide latest version and license of operating system, Anti-Virus or any other software delivered in the project at its own cost. If changes of software and operating system require replacement of hardware's, then, hardware shall also be replaced by the contractor without any cost implication to owner. Replacement shall be of either same or higher configuration keeping required performance specified under the contract and from same OEMs.
- Contractor has to provide latest version of SCADA/EMS Application software before the start of Site Acceptance Test (SAT) without any cost implication.
- If any development, customizations, testing, etc. needs to be done for the compatibility of SCADA/EMS and other applications on the new OS platform, Anti-virus and any other software delivered in the project upgradation, then the same shall be done by the contractor at its own cost.

4.2.3 Commercial Off-The-Shelf (COTS) product

Commercial Off-The-Shelf (COTS) product means bidder has to quote product which is independently commercially available in the market. For all such products bidder has to provide at least three references in Govt/Public Listed companies at the time of bid submission and same shall have been sold as an independent product and solution shall be in successful operation for at least three years **at the time of bid submission.**

For that Bidder has to submit copy of PO/LOA and installation/completion/**operational** certificate **issued by the Customer** for the relevant reference.

4.3 Time and Calendar Feature

The SCADA/EMS system shall maintain Time and calendar for use by various software applications. A NAVIC (with fail back option to GPS) based time reference shall be used for synchronizing the SCADA/EMS system time periodically. The internal clocks of all Servers and workstation consoles shall be automatically synchronized within the accuracy of +/-100 milliseconds of synchronized time on NTP or PTP protocol. The calendar shall be customizable for working hours, holidays, weekends etc. Suitable alarm shall be generated on failure of any of the sources/receiver of GPS in SCADA/EMS system.

The SCADA/EMS system shall include two redundant time and frequency receivers. Failure of the online unit shall result in automatic switching to the redundant unit. The SCADA/EMS shall periodically check if the backup unit is operational and failure of either unit shall be alarmed.

The Contractor-furnished NAVIC (with fail back option to GPS) based Time facility shall be read and compared to the time and date maintained by the time and calendar function at least every fifteen minutes and when a SCADA/EMS or any other system is initialized. If the time and frequency facility is available and the two times are within a user adjustable dead-band, the SCADA/EMS time shall be set to the facility time. If the two times differ by an amount greater than the dead- band, the SCADA/EMS time shall not be updated and an alarm shall be generated. This time difference shall be alarmed every 15 minutes if not corrected.

The user shall be able to alter the date and time. The day shall be in DDMMYY/DDMMYYYY format. The alteration shall not adversely affect programs running at the beginning of the hour. The function shall enable day calculation e.g. Day of the week/week of the year for reference for any display.

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/EMS system shall include software for network communication and network services. Network software shall include the user node software that provides the connection of that node to the network. The network node software shall be provided for each type of network node connection supplied with the initial system and shall be licensed for the quantities and types of nodes defined for the SCADA/EMS System configuration.

It should be able to generate reports for a defined period regarding availability of communication links. In case any communication link is DOWN/OUT/Failure then a pop-up should come up for it along with the SMS and e-mail facility shall be implemented for the same.

4.4.1 Network Communication

Users and various applications shall be able to communicate within the SCADA/EMS system 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 such as local and remote workstations, servers, and peripheral devices into a common data communication network allowing communications among these devices.

4.4.2 Network services

The following network services shall be provided for the users of SCADA/EMS system within the LAN if not in conflict with security requirements:

a) File management and transfer of files containing text, data, and graphics information
b) Network printing management
c) Network time synchronization
d) Backup over LAN (Storage Area Network)
e) Task-to-task communications to external computers
f) Remote procedure call
g) Remote terminal session

4.5 Network Management System (NMS)

The Network management system shall facilitate following activities: -

a) Security / Monitoring to protect systems and network from unauthorised access, manage user access, authorising rights and privileges

b) Inventory Management to collect information about computers in the system such as processors, memory, peripherals and processes running on computers and provide network map of interconnected equipment in LAN/WAN. All IP based devices in network should be monitored.
c) Performance Management to monitor system and network performance as specified
d) Fault Management to recognize, log and identify fault on network and connected machines, nodes, devices.
e) Preferably centralize and consolidate events from various disparate monitoring

tools.

f) Facilitate as universal interface to determine and resolve IT issues quickly across servers, storage, network and Workstation.

The network management software shall be based on the secured version of Simple Network Management Protocol. The NMS system shall have a user-friendly browser-based user interface to provide all the pertinent information about the system. The NMS shall not impact the availability and performance of SCADA/EMS system and shall load **not more than 3% any host CPU**, **1% Network bandwidth** and shall have secure communication.

The Network management system shall monitor from single dashboard and correlate the performance, connectivity, resource usages and error statistics of all the servers, workstations, routers and LAN devices including proposed Owner networks extension (**up to 100 number of nodes**) including the following: -

a) Utilization (CPU and/or channel time being used as applicable) for
    a. **All the active devices** (Servers, Workstations, Storage Devices (SAN, NAS, HDD etc.)
    b. Router, Switches, **Firewall etc.**
    c. Data Links **(bandwidth utilization of current and last 24 hours)**
b) Memory utilization, Auxiliary memory I/O utilization, of
    a. **All active devices** (Servers, **Workstations,** and Other Machines)
    b. Mass Storage Devices
c) Temperature monitoring of **all active devices** (servers, network and storage devices etc.),

The Network Management Software shall: -

a) Maintain performance, resource usage, & error statistics and present this information via displays, periodic reports, and on- demand reports.
b) Apart from real-time monitoring, the above information shall be collected and stored at user configurable periodicities **i.e., 5 minutes to 60 minutes**. The Network Management System (NMS) shall be capable of storing the above data **for a period of one year at a periodicity of 5 minutes**. NMS shall be able to generate reports regarding utilization of RAM and CPU. Export of this data shall be provided in ".CSV", ".XLSX", etc. formats.
c) Maintain a graphical map display for connectivity and status of servers and peripheral devices for local area network. Issue alarms when error conditions or resource usage problems occur. Graphical display should indicate change

in status of device or interface in color and blinking. NMS shall automatically discover the equipment to construct the afore-mentioned map.

d) It shall support management of all network hardware, printers, servers, storage and workstations etc. (envisaged in this technical specification) irrespective of platform/make.
e) Issue alarms when error conditions or resource usage problems occur.
f) Report on application, server and network events from a single console, for faster triage and diagnostics, compliance to provide the IT search and intelligence analytics.
g) 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.
h) The statistics shall be available for printout and display after each period and on demand during the period.

4.6 Database Development Tools

The Contractor shall provide all necessary software tools for the development and maintenance of the SCADA/EMS System (SCADA, EMS, PSA (Power System Application Database), DSA, AGC, ICCP, Historian, Web Report, etc.) databases at Control Center.

Each database shall also have separate description field (different from ID field) against each record which shall sufficiently large enough to accommodate description of the record field enterable by the user. This field will be used for creating informative display for system operators and SCADA system administrators. Automatic ICCP names creation with inherent linking of SCADA/EMS database shall be available with database development tool. Database development shall be done in consistent with Guidelines on Naming Convention in SCADA database at Load Despatch Centres (**Part-B Appendix O**).

This tool shall be capable of managing the entire system database. The database development software tool delivered with the SCADA/EMS system shall be used to generate, integrate and test the database. The background color of database tool shall be user configurable.

The database development tool delivered with the system shall be user friendly. The database development tool shall facilitate IEC 61970 and CIM data exchange of both incremental and full power system model. CIM compliance shall be provided amongst the CIM version of existing control centres.

The database tool should have facility to export and import model files (both Full and Incremental) as per IEC 61970 part 552-4. The product should have facility for exchange and transformation of Power System Model files including Generation and Load through execution of Power flow applications. The following instance data shall be included in the above said exchange:-

- Generation Values
- Load Values
- Measurements
- Transformer Settings
- Generator voltage control values
- Device States
- MVAr Values for Shunt Compensators

This tool shall contain database structure (format) definitions and all initialization data to support the generation of all relational and non-relational run-time databases required to implement the system's SCADA/EMS functions. The tool shall include consistent, coordinated procedures to manage and access the databases regardless of the location of the data or the residency of the database management functions within a control centre. All exchange, coordination and procedure required across a control centre shall be independent of each other. This tool shall allow following modes.

- **Incremental data exchange of a function**

This tool shall be used to exchange the incremental modeling of SCADA, ICCP, FEP, DSA models with proper validation of topology, field data and modelling errors.

- **Complete data exchange of a control centre**

The data exchange shall be possible in different time frame and shall not impact the ability of Control Centre to make changes in online database.

This tool shall include definition of data fields, structure of application data sets using the global database, database population, correction of entry errors, checkout against telemetry definitions for SCADA functions, checkout against model definitions for power system analysis functions.

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. Help displays shall be available to provide additional, detailed information to the user on request.

Database development and Display tool shall be accessible from all the workstations without any limitation supplied under the project and user can work on it concurrently.

4.6.1 Symbolic Access

Interfaces to all SCADA/EMS databases shall be provided through the facilities of the system's high-level programming languages. Database items shall be identified by symbolic names when the database items are defined. Subsequent references and linkages to any database item shall use these symbolic references. Each database item name shall be unique. Programmer shall only have to define this item once to establish all internal database linkages to this item's attributes when creating the database.

A software search utility shall be provided that will list all the displays and calculations where a user specified database item is used. The list display shall facilitate invoking relevant tool to modify the point or change the calculation or access the applications or calculations that will be affected by deletion of the point.

4.6.2 Database Management

The database manager shall locate order, retrieve, update, insert, and delete data; ensure database integrity; and provide for backup and recovery of database files. The database manager shall generate and modify all SCADA/EMS data by interfacing with all database structures.

In systems with a distributed database, the database manager shall have access to all portions of the database wherever stored. The location of database items shall be transparent to the user performing database maintenance.

Execution of the database manager in any server of the system shall not interfere with the on-line functions of the SCADA/EMS including the normal updating of each server's real-time database. In a primary server, database editing shall be limited to viewing functions, database documentation functions, and functions that change the contents but not the structure of the database Editing the on-line database shall not affect the operation of the primary/backup configuration.

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 initialize 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.

The database manager shall include the mechanisms, in both interactive and batch processing modes, to perform the following functions:-

- Add, modify, and delete telemetered, non-telemetered, or calculated database items and data sources such as data links, and local I/O.
- Add, modify, and delete application program data.
- Create a new database attribute or new database object.
- Resize the entire database or a subset of the database.
- Redefine the structure of any portion of the database.

A utility function shall be provided that creates, from the run-time database, a source file suitable for submittal to the global database batch processing facility. This utility shall create a new global database file, suitable for editing, that reflects any changes made to the run-time database since the last time the database was generated.

ICCP association with other control centers shall be made simultaneously and automatically irrespective of the cause such as on lining, Communication failure, dataset failure, software failure at either of the ends.

Modelling of elements for SCADA, Network Applications and DTS may be different and the database Administrator shall have the options for above modeling.

EMS database creation should have feature to show node breaker model for station and bus-branch model for entire database showing connectivity between the stations.

EMS database manager should have graphical modelling functionality to link the elements with its nodes and the node records should get created automatically with the database.

Database Management must have validation tool for each type of databases SCADA, DSA, ICCP, EMS and AGC database with field/point specific validation checks considering integrity between the database.

Database Manager should have functionality to maintain any types of user defined model for dynamic model creation for elements (Thermal and Hydro generators, Renewable generators (Wind, Solar etc.), Load dynamics) which should be consistent within DTS and DSA databases.

Attributes for area and discom wise shall be defined in database hierarchy so that area wise/district wise /city wise load display could be made using these attributes.

4.6.3 Run-Time Database Generation and Maintenance

The database manager shall generate incremental database changes as well as run-time (loadable) databases from the global database. Based on the nature of the structure change, the database management software shall determine which portion of the database must be regenerated and which displays, reports, and software functions must be re-linked.

When errors that were not detected at data entry time are encountered during run-time database generation, these errors shall be flagged. The generation routines shall attempt to continue processing the database in an effort to detect all existing errors before terminating the generation task. The feature for sorting/filtering the error based on type and severity level may be included. The error report should have the prompt for guidance for corrective action. A document regarding the various errors that may occur during database creation or modification and the possible reasons and methodsfor alleviation need to be provided.

4.6.3.1 Data Retention

The database generation process shall retain and utilize data from the current SCADA/EMS 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.

4.6.3.2 Database Integration (on lining)

Newly generated run-time databases shall only be placed on-line by user command. After an error-free database generation, the new database shall be integrated into the system by assigning it to an appropriate 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. Following the assignment of a new database to a server and on user demand, the database management software shall access each SCADA/EMS server to ensure that all databases are consistent. Inconsistencies shall be annunciated to the user. **Further, appropriate message/alarm shall be generated after the on-lining of each relevant application/database.** The database changes made in Main Control Center shall be reflected immediatelyin Backup Control Center with minimal user intervention and without requiring any downtime.

At regular intervals (Daily) the database of Main and Backup Control Centers be checked for any differences in entries, linkages, calculations and database elements and necessary updation shall be done for the same.

It shall be possible to do Database Integration by following method:

- **Real Time - No Failover of Online Server required.**
- **Off Line- Failover of Online Server required.**

Databases for all Application like Web, Replica server/Historian should be updated automatically.

4.6.3.3 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, database documentation functions, and changes to the contents, but not the structure of the database. On-line changes shall be implemented in all applicable SCADA/EMS run-time databases without requiring any downtime of the system. 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/EMS system's reaction to hardware and software failures nor shall it require that the exchange of data among servers for backup purposes be suspended. The On-line editing of database and its backup to standby machine should not result into the failover of servers. There shall be no loss of connectivity to the client workstation as well as real time data loss or non-availability during editing either in main or backup servers except the corresponding station data till the final editing and committing the database.

4.6.3.4 On-line editing of SCADA, ICCP, FEP, DSA, AGC and EMS databases

Online editing of SCADA, ICCP, FEP, DSA, AGC and EMS databases shall be made available to the user. Proper User Interface for online editing (without involvement of server failover or re-start) of these databases. For ICCP database, mapping with individual control centre along with its editing shall also be provided. Similarly, for other databases online editing could be possible for users.

4.6.4 Tracking Database Changes

The database manager utility shall maintain Audit trail files for all changes made by all users including on-line database editing. 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 last 10,000 edit operations shall be maintained. User shall be able to compare two cases of database at any point of time.

4.6.5 Initial Database Generation

The Contractor shall be responsible for the initial database generation afresh by using data available at control centre in association with the Owner. The Contractor shall arrange the required software tool to acquire the initial data from the existing control centre at his own cost. The owner shall provide the access to these control centres for acquiring the required data. However, the software tool shall not degrade the performance of existing system in any manner.

4.6.6 Development System (DDS or PDS) as a test bench

A Test bench i.e., PDS shall be delivered by the Contractor with capability of replicating any SCADA functionality (ICCP/SCADA/FEP) in online mode and shall be provided in both in Main & Backup Control Centre.

The PDS shall be able to re-create any SCADA functionality for online/offline testing and development; it shall be loaded with replica(s) of SCADA, ICCP, FEP Servers and 03rd party software(s) configured in the deployed environment. Database Development system is one of the important component and contains entire off-line database of the system, any mistake/loss may impact entire system.

Hence, one separate database test system has been envisaged. This test Database Development System shall be able to provide testing facility for integration of new RTU and new Control centre with Main and Backup SCADA/EMS system before putting it online with Real-time system.

The development system synchronization with real time database shall be simplified.

- **Integration of New RTU**: Development System shall be used to test the integration of new RTU on all RTU protocols as envisaged in the specification.It will facilitate in validating all the functionalities of the SCADA as explained in earlier sections.

It shall be possible for the development system to run in a 'listen' mode whereby the data exchanged between the online system and field RTUs simultaneously updates the database on the development system. This is to facilitate testing of pending database changes on the development system without interfering with existing communications on the online system.

Testing of Integration of new control Centre on ICCP protocol: Test Database Development System shall be used to test the integration of new Control Centre on ICCP with Main and Backup Control Centre. Development System shall have the capability of modelling new ICCP connections for both Main and Backup Control Centres.

In test bench mode, Development System shall be able to connect through the existing LAN/WAN to the new RTU and/or Control Centre and test the link step-by-step as well as continuous run mode up to 24 hours to observe the data acquisition/exchange process.

During the continuous run mode, the data collected shall be stored in a temporary files /tables for review to assess effectiveness and stability of integration. All relevant logs for monitoring the communication with RTU & Control Centre under test such as defined for regular SCADA/EMS system shall be stored and presented/reported on similar displays. The Hardware required for necessary connectivity including the interface with communication links shall be included as part of Database Development System (DDS) Hardware.

- **This system shall also be used as a Test bench for Cyber security** and shall accordingly be equipped with firewall, antivirus and enable mode wherein threat scenarios can be tested with configured security elements before implementing on the main/production system.

This Test bench for Cyber security shall also be used for VAPT (Vulnerability Assessment & Penetration Tests) e.g. OS fingerprinting, Port scanning etc. In test bench mode, Development System shall be able to connect through the existing LAN/WAN to the new RTU and/or Control Centre and test the link step-by- step as well as continuous run mode up to 24 hours to observe the data acquisition/exchange process. During the continuous run mode, the data collected shall be stored in a temporary files /tables for review to assess effectiveness and stability of integration.

All relevant logs for monitoring the communication with RTU & Control Centre under test such as defined for regular SCADA/EMS system shall be stored and presented/reported on similar displays. The Hardware required for necessary connectivity including the interface with communication links shall be included as part of Development System Hardware.

4.6.7 CIM (Common Information Model- 61970) compliant Data Modelling Import & Export Tool

The Contractor shall provide Database import and export tool, which shall be CIM compliant. This tool shall be repository of RLDC data model and shall facilitate exchange of data model across control centers (NLDC, SLDC Other LDCs). A user-friendly UI shall be provided to extract/transform/load; as required; model data/parameter/devices for interchange with LDCs. The Import & Export Tool shall have feature of searching, sorting and merging on parameters/devices/nodes /company's including that of power system.

It is desirable that the tool facilitate identification and search of nodes/telemetry points/ values to be exchanged from a given LDC. The tool shall be able to import & export different versions of CIM.

Owner is in process to establish centralized database system which will be CIM complaint. User will have access to this database and shall model required component in this centralized database. Subsequently related database shall be extracted and imported in this proposed system. Contractor shall be responsible to develop CIM tool which shall be able to exchange the files from this database in CIM format.

The tool should be capable of importing and exporting data in PSS/E formats, alternately separate utility shall be provided for the same.

Tools shall have following capability:

During Upgradation of SCADA/EMS: It shall Import/export database from existing SCADA/EMS system in CIM format (latest version with backward compatibility).

During Maintenance of SCADA/EMS: It shall Import/export database CIM format (latest version with backward compatibility) with other control centre.

An integrated CIM Import module shall be provided which will be capable of building power flow data from CIM in either bus/branch or node/breaker format. The module shall be made to support both off-line and on-line power flow analysis including dynamic security assessment (DSA) tools.

The Import module shall follow these standards to extract and build power flow data from CIM –

- IEC 61970 (Energy Management)
- IEC 61968 (Distribution Management)
- IEC 62325 (Service Oriented Architecture)

The CIM Import module shall consider the following data from the above standards –

- **Equipment:** all network components defined in the supported CIM versions shall be included in the power flow case.
- **Topology:** the resulting power flow case shall be based on the bus/branch format. The node/breaker model shall be added if data is provided.
- **Steady-State Hypothesis (CIM16+):** status of all network components, as well as generation and load values, shall be extracted and included in the power flow case so that a flat power flow solution can be performed.
- **State Variable:** bus voltages, shunt settings, transformer tap ratios, etc. shall be obtained for power flow solution and analysis.

Applications: The CIM Import module shall be used for a variety of applications, including the following as a minimum –

- Power flow analysis.
- **Topology analysis**: the CIM Import shall have a feature to enable it to collapse buses connected by breakers/switches so as to reduce the zero impedance lines in the resulting bus/branch model.
- All network components shall have equipment names assigned in the power flow case.

4.7 Display Generation and Management

The Contractor shall provide necessary software tools preferably browser based for the generation and management of SCADA/EMS displays for both SCADA/EMS system. Display fit, with proper utilization of space, clear visibility of analogs in display fit also with least unused space shall be provided. Utility to import & export displays through DXF or DWG or XML format (latest version with backward compatibility) from other control centers shall be provided.

SCADA/EMS displays shall be generated and edited interactively using this display generation software delivered with the system. The display generator and management features specified in the following paragraphs shall be available at the workstation console.

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/EMS system shall be provided. All libraries shall have directories that list all elements contained in the library. These directories shall be displayable and printable on demand. All libraries shall include a library compression facility that consolidates unused space created by removal of old elements to allow efficient reuse by added elements. Displays shall be generated in an interactive mode. The user shall be able to interactively:-

- Develop display elements
- Link display elements to the database via symbolic point names
- Establish display element dynamics via database linkages
- Define linkages to other displays and programs
- Combine elements and linkages into display layers
- Combine display layers into displays.

Execution of the display generator functions shall not interfere with the on-line SCADA/EMS functions.

All workstation features and all user interface features defined in this Specification shall be supported by the display generator software. An audit trail of all interactive generations and edits shall be maintained by the display generator software. An audit trail of last 10,000 edit operations shall be maintained.

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.

The display editor/generator shall have option to compile all displays corresponding to a change in a symbol or element in the library.

For Display Generation, the contractor shall following display building guidelines, as mentioned in **Appendix K.**

4.7.1 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. These Dynamic Transformation Linkages should be configurable for each of the individual displays and functioned accordingly.

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/EMS 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, a DXF formatted file imported from another system, or an existing display. Graphic display shall consist of multiple display layers. 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 a partial display. To protect against loss of display work when a server fails, the current work shall be automatically saved every five 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. 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.

The display created in display generator shall be updated across the SCADA/EMS applications. The display generator shall support various fonts, font-types (Hindi, regional languages etc.). The display generator shall have editing options such as cut, copy, paste etc.

The display once verified error-free from the display generator; shall be integrated directly into all functions namely: DDS, SCADA, EMS, DTS, Replay/Payback, and WEB directly from the display generator in a single step.

The display generator shall be fully compatible with all SCADA displays and shall follow the concept of WYSIWYG (What You See Is What You Get). The layer mapping should be proper. The display generator shall support various fonts, font-types (Hindi, regional languages etc.). Menu based EDIT facilities (cut, copy, paste from same or other displays) shall be present in the display generator.

4.7.3 Import/Export CADD Drawings

The display generator shall support the import of drawings, including power system one-line diagrams, developed by Employer/Owner on Auto CAD. The display generator should have the capability to import the files from latest version of AUTOCAD including older versions for display generation. Further the drawings may also be used in the SCADA/EMS system as the static background for displays. The display generator shall provide the capability (through the display generation process), 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/Owner 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.

The display generator shall also have facility to export the SCADA/EMS displays in XML or DXF or DWG format (latest version with backward compatibility) to be used in AUTOCAD.

For DXF, DWG, XML, AUTOCAD it should support latest version with backward compatibility.

4.8 Software Utilities

Some of the software utilities, which are required to be delivered along with the SCADA/EMS system, are described here. However, Contractor shall supply all software utilities used to develop and maintain SCADA/EMS software, whether or not specifically described by this Specification, but, requires to meet the various functionalities specified under this technical specification.

The software utilities shall operate on-line (in background mode) without jeopardizing other SCADA/EMS application functions those are running concurrently. Utility software shall be accessible from workstations, processor terminals and servers.

4.8.1 Backup System

Utility to take backup of auxiliary memory files of server, workstation, database onto a user-selected archival device based on supplied system by the Contractor. 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.
(e) Image Backup
(f) Incremental Backup

The utility shall also take image backup daily automatically on backup appliance. It shall keep minimum two (02) set of image backup of all servers and one image backup of all the workstations on backup appliance (along with other backup details mentioned in Appendix-H, PART-B) and another Two (02) copies shall be maintained, out of which one shall be maintained by Contractor on SAN/NAS and other with Owner on external hard disk. Each day it will take image backup, when image backup is successful then it will delete the oldest image backup. It shall be possible to archive these image backups on external hard-disks. Bidder shall supply online agents (if required) for image backup of all the servers, workstations, databases etc.

Automatic full or incremental back up capability of selected systems at user-defined intervals shall be provided. It should be possible to restore or recover any software/system at a selected time form backup.

User shall be able to archival of backup data on external hard-disks and utility shall be able to archive data automatically on SAN/NAS and external hard-disks as per the user defined schedule.

The utility shall allow restoration of the servers/workstation from the image backup without requiring any other software. Any server restoration from image backup shall take less than 2 Hours. Minimum speed of restoration shall be 200 Giga-Byte/Hour. Detailed scope and Technical specification of proposed backup appliance along-with required features, SAN, NAS etc is mentioned in **Appendix-H**.

4.8.2 Image Backup and Restoration Utility for Networking devices

Running configuration image backup (automatic) for each of the Networking equipment (Routers, Switches), Firewalls used in the system should be made available in NAS/SAN/backup appliance as well as in portable hard disk as per user defined periodicity. The utility shall also have the capability to restore the configuration of devices.

Application shall be provided to store configuration of Routers and Switches. For the Firewalls, configuration shall be stored in centralized management application of OEM.

4.8.3 On-Line Monitoring Diagnostics

On-Line monitoring diagnostic programs shall be provided for verifying the availability of the backup equipment and for limited testing of devices without interfering with on-line operations of the SCADA/EMS system or the failover capability of the devices.

Redundant communication line interface equipment shall be tested by periodically retrieving data over these lines and checking for the ability to communicate with the redundant channel and for any errors.

Designated backup server(s) and associated auxiliary memories shall be automatically tested for proper operation to ensure they are ready if needed for a fail over contingency. Any failure to perform diagnostic functions correctly shall cause an alarm to be issued.

4.8.4 Document Management System

a) Web based "Document Management System" (DMS) software shall be supplied and installed at the owner's facility by the contractor along with minimum 50 number of client access licenses and minimum 10 concurrent users.

b) The DMS shall be complete system to be used for management of documentsincluding group editing, versioning etc.
c) It shall have complete capability of tracking the documents version, ownershipand editing.
d) It shall have web-based user interface (accessible from any client through browser) hosted on a server with backend independent database.
e) DMS shall store and make available the all documentation of the project.
f) It shall have the facility for version control, access control, archiving etc. Allaccess to the document shall be based on the privileges assigned to the user.
g) DMS shall have multiuser capability with user role and privileged management.Complete user management system along with predefined roles shall be in
h) built in the DMS.
i) DMS shall be used as central document repository for the entire lifecycle of theproject for easy managing and referencing of the project documentation.
j) The Document Management System shall have a facility to integrate the Owner's made documentation for system Operation to be used by Operator.

4.8.5 Data Exchange Utilities

Facility of data export and import from and to SCADA/EMS system to external system in a secure manner ensuring latest cyber security guidelines issued by statutory authority from time-to-time shall be provided as detailed below: -

Through OPC Server: A full OPC server compliant to the latest standard shall be provided in order to export real time data, alarms, historical data etc. to the external system. Authentic OPC server and clients for WINDOWS and Linux shall also be supplied as per BoQ which shall be installed in external system and shall exchange data with OPC of SCADA/EMS system. If client software is based on the user system then minimum no. of user license as specified in BoQ for each shall be provided. The server shall be licensed accordingly.

Through ODBC/JDBC: Capability of export of SCADA data to external system though ODBC and JDBC shall be provided. All system parameters in the real-time database including real time data, calculated data, application configuration parameters and application output shall be available through the ODBC interface. Limitation if any or pre-requisite on PC for use of this interface, shall be clearly defined. It shall be possible to export data through SQL queries to external system.

Through SOAP and REST: The SCADA system shall provide web services on

SOAP and REST that allow multiple applications to exchange any data points including alarms and events

Injection of external values: Suitable facility of injecting values form external system to SCADA database should be provided. API along with utilities shall be supplied to facilitate this feature. It shall be provided to inject external values to SCADA Database over periodic intervals and in real-time. It should be possible to use this API for developing the programs on Windows or Linux system using programming languages and macros.

4.8.6 Other Utility Services

The SCADA/EMS shall include the following utility services:-

- Loading and storage of information from labelled portable media storage units as dictated by the requirements of this Specification.
- On line access to user and system manuals for all software products (e.g. Operating System and Relational Database Software) and SCADA/EMS applications shall be provided with computer system.
- The contractor shall provide licensed utilities for preparing the .pdf output for the displays/reports available in the SCADA/EMS system. PDF creation shall be of entire display not the screen portion only. It should also be possible to export all such reports to MS-Office format (like MS word, MS excel and PDF etc). The MS office software and Adobe-PDF **reader** (With Valid License Version) software shall be provided in each of the workstations, laptops and remote consoles by the contractor).
- The contractor has to supply MS Office and **Adobe** PDF **reader** software (With Valid License Version) for all the supplied endpoints (workstations, laptops, CPU, remote consoles etc).
- The contractor shall provide the provision for SCADA display files to be saved in jpeg, pdf, rtf file format and also selected displays to be saved in jpeg file for every 1 minute.
- The SCADA displays shall have the capability to be printed to pdf format on a schedule multiple times (5-6 at least) a day, without manual intervention.
- **Displays and Reports for Web server -** The Contractor shall provide utilities for preparing displays and reports suitable for Web publishing. These utilities shall be used to generate, all required displays and reports from the SCADA/EMS system displays and reports, automatically (without requiring rebuilding).
- A tool shall be provided to extract/export of all the real data (analog, status

etc.) for any instance selected by user.

• A tool/script for automatic snapshot of selected displays (max up to 20) shall be provided at user selectable interval

4.9 Virtualisation

Virtualisation technique uses software to create an abstraction layer over computer hardware that allows the hardware elements of a single computer—processors, memory, storage and more—to be divided into multiple virtual computers, commonly called virtual machines (VMs). Each VM runs its own operating system (OS) and behaves like an independent computer, even though it is running on just a portion of the actual underlying computer hardware.

Virtualisation techniques enables more efficient utilization of physical computer hardware and allocation of resources as per the requirement over the period of time. Accordingly, Virtualisation techniques has been considered under the project for many applications as per the proposed architecture. This also facilitates in reduction of number of physical servers at-the same time providing more reliability.

Virtualization brings several following benefits:

- **Resource efficiency:** Server virtualization allows to run several applications—each on its own VM with its own OS—on a single physical computer without sacrificing reliability. This enables maximum utilization of the physical hardware's computing capacity which can be allocated to the VMs as per the requirement.
- **Easier management:** Replacing physical computers with software-defined VMs makes it easier to use and manage policies written in software. Policies can even increase resource efficiency by retiring unused virtual machines to save on space and computing power.
- **Minimal downtime:** OS and application crashes can cause downtime and disrupt user productivity. Redundant virtual machines can be configured and failover between them can be configured when problems arise.
- **Faster provisioning:** Buying, installing, and configuring hardware for each application is time-consuming. Provided that the hardware is already in place, provisioning virtual machines to run all your applications is significantly faster.

-----End of section4-----

Section 5

Hardware Requirements

Table of Contents

Section 5 Hardware Requirements

5.1 General Requirements

This section describes the technical requirements of all the hardware envisaged in the BOQ for the SCADA/EMS system. The minimum hardware specifications (RAM, Aux. Memory, interfaces etc.) for all equipment are specified in **Appendix- H of Part- B** and the bidder have to submit the details of the supplied hardware along with the bid as per format attached in **Appendix- H.** The Bidder shall asses the adequacy of hardware specified in the BOQ & if any additional hardware or higher end hardware configurations are required to meet all the requirements of the technical specifications, the same shall be included in the offer. The Bidder's proposal shall include necessary calculations to clearly establish that the proposed hardware meets the functional and performance requirements of the technical specification.

The bidders are encouraged to optimize the requirement of hardware for servers and processors where one or more applications can be combined or distributed in any combination with adequate redundancy. However certain applications are to be hosted on independent hardware.

5.2 Technical Requirements for Hardware

All hardware shall be manufactured, fabricated, assembled and finished with workmanship of the highest production quality and shall conform to all applicable quality control standards of the original manufacturer and the Contractor. All hardware components shall be new and suitable for the purposes specified.

All hardware shall be of reputed make. All hardware shall include self-diagnostic features. On restoration of power afterinterruption they shall resume operation. All servers, workstations and network equipment (Switches, routers, firewall etc.) shall be compatible for remote monitoring using secure SNMP (latest version). All hardware shall support both IPv6 and IPv4 simultaneously.

The contractor shall ensure that at the time of final approval of hardware configuration and BOQ, all the hardware is as per the current industry standard models and that the equipment manufacturer has not established a date for termination of its production and consumables e.g. printer cartridges, are available with more than one supplier locally.

All hardware shall be of reputed make and meeting the following criteria:

a) All equipment shall be IPv6 ready from day one; requisite licenses, etc. for the same shall be included in the quoted price. The entire system shall be configured on IPv6 with suitable NAT64 provisions at the gateway level.

b) All the Equipment provided under this contract shall be supplied with 3-pin, 5A OR 15A plug tops complying with Indian Electrical standards. The Equipment shall operate on 230 volts, 50 Hz single phase AC power supply.

c) The Equipment to be supplied under this contract shall be the industry proven products and not the R&D models. The equipment shall confirm to the requirements of relevant Indian & International Standards.

d) The Bidder shall ensure that product/technologies/services quoted under this project are latest and it shall have more than 7 years of life initially (i.e.., "End of Support Life" for minimum 7 years, from date of bid submission) which shall be extended during entire contract period (including extension of contract, if any) by extending the OEM warranty or replacing the product.).

e) Proposed hardware offered by the OEMs shall be of the same series which have at least three references in Central / State Govt Organization / PSU / Public Listed Company as on the originally scheduled date of bid opening. For that Bidder has to submit copy of PO/LOA and installation/completion certificate for the relevant reference.

f) Assembled products of different makes or refurbished products shall NOT be accepted (Example: In case of computer system like Monitor, Keyboard and Mouse).

g) The BOQ estimated by Employer/Owner is NOT exhaustive. Any additional items/ components as required for the successful completion of the work undertaken may be assessed by the Bidder and the same may be incorporated in the offer. The BOQ as assessed by the Bidder as above shall be clearly indicated in the offer. Even at the time of execution, if any additional items/components are required to complete the system, notwithstanding the BOQ as identified by the party as above, the same shall be provided free of cost by the Bidder.

h) All the supplied system shall be under OEM (Hardware and Software) warranty & support till the completion of entire AMC period (including extension of contract, if any).

I) During entire contract period (including extension of contract, if any), if OEM discontinues/ ends support to any item supplied (software/hardware/security solution) under the contract, bidder has to replace such hardware, software (or both, depending on software or hardware dependency) without any additional cost to Owner. Replacement shall be of either same or higher configuration and from the same OEMs.

j) Price of all the client licenses shall be included in end-point equipments (laptops, Workstation etc.) for which unit prices has not been asked in BoQ separately, in case of quantity variations only hardware prices will be considered.

Any hardware changes, except version upgrade in same series, proposed after contract agreement shall be subject to the following: -

a) Such changes/updates shall be proposed and approval obtained from Owner along with the approval of Drawings/documents.

b) The proposed equipment shall be equivalent or with better features than the equipment included in the Contract from same OEM.

c) Complete justification along with a comparative statement showing the original and the proposed hardware features/parameters including brochures shall be submitted to the Owner for review and approval.

d) Changes/updates proposed will be at no additional cost to the Owner

e) The porting of software shall be at no additional cost in case of replacement of hardware during the AMC period by Owner in consultation with contractor.

5.3 Hardware Configuration

In this technical specification all hardware has been broadly classified as "Server" and "Peripheral device". The term "server" (also referred as "processor") is defined as any general-purpose computing facility used for hosting application functions as defined in the specification. The servers typically serve as the source of data, displays and reports. The term "Peripheral Device" is used for all equipment other than servers. Peripheral device includes Workstation consoles, WAN router, LAN, printer, Time & Frequency system, storage device, External Cartridge, Magnetic tape drive, VPS, Firewalls etc. **and other devices/solution supplied under the project.**

The redundant hardware such as Servers, Firewall, and LAN etc. shall work in hot standby manner. All the servers and networking equipment (Firewalls, LAN equipment, etc.) shall be mounted in rack panel. Grouping of Network equipment in a rack shall be such that the primary and backup network equipment or a system function are located in different racks. The Typical hardware configuration is attached at **Appendix- D of Part -A. The connectivity between networking devices shall be designed having mesh connectivity.**

5.4 Servers (Rack mountable servers)

The Servers shall have provision for **upgrade** of the processor, auxiliary memory and Main memory (RAM) as mentioned in technical specification. This expandability shall be possible at site with addition of plug-in modules. Initially USB ports of all servers/work stations shall be disabled.

Rack Mountable Servers: Servers shall be mounted in a rack (panel) and a rack mountable TFT monitor, keyboard and mouse using an IP based KVM switch to access all servers & peripherals in the panel. Further, a server management console shall be installed at owner decided location to access all servers centrally. Each KVM switch shall have minimum 16 ports. However, the groupingof servers in a rack shall be such that the primary and backup servers for a system function are located in different panels.

All servers shall have dual redundant power supplies, capable to operate on single power supply module. And there shall not be any interruptions in the operation of servers when there is a failure of either one of two AC Power Supply of the server. All servers shall be hot swappable, dual redundant power supplies and be capable to operate on single power supply module. And there shall not be any interruptions in the operation of servers when there is a failover between the two AC Power Supply of the server. Servers supplied shall be compatible to connect with the external storage and other network components identified in the BOQ, necessary additional hardware (if any) required for connectivity shall be part of servers.

Some of the applications shall be installed on physical server whereas many shall be on virtual servers as per the proposed architecture and bill of quantity. Accordingly, servers shall be supplied with the virtualization software to create the virtual machines. Configuration of Servers and Applications shall be configured as per the proposed architecture (as a critical and non-critical). Non-critical applications shall be distributed between redundant physical servers for proper utilization of both the physical servers.

5.5 CFE (Communication Front-End) Server

The CFE server offloads the task of communication & pre-processing between RTUs (on both IEC 60870-5-101 and IEC 60870-5-104 protocol, OPC, Modbus etc.,) & terminal servers and SCADA/EMS servers. All RTUs shall be connected to redundant CFEs. RTUs are connected to CFE through different communication medium via interface. The interfacing hardware such as splitters routers, LAN, firewall shall also be housed in the CFE cubicle preferably. CFEs shall have a suitable interface for time synchronization from the GPS based time synchronizing system. This interface shall have the time synchronization accuracy of 1 millisecond. The CFE shall further synchronize the time of the RTUs on IEC 60870-5- 101 protocols. Each RTU shall be connected to both the CFEs through a splitter, unless a RTU has a redundant communication channel. In case of noise in RTU, the CFE functioning or functioning of other RTUs in the same channel should not be affected. Logs for each RTU shall be available in the browser/GUI display and Sorting, filtering features shall also be available in display.

The CFE shall be provided with suitable interfaces for communication with the RTUs over IEC 60870-5-104 protocol, OPC, MODBUS etc., One set of Router cum firewall for RTUs shall be provided between RTUs and CFE for RTUs communicating with control center on IEC60870-5-104 protocol as per the BOQ. However, all the data from field to CFE shall be routed through internal Firewall.

5.6 RTU communication over IEC 60870-5-101

The CFE shall have sufficient number of V.24/V.28 interface boards for communicating with the RTUs on IEC 60870-5-101 protocol. The number of V.24/V.28 ports in each CFE shall be adequate to integrate the specified no. of RTUs and shall have spare ports. The CFE shall support RTU communications by interfacing with the RTU over various media such as power line carrier, leased line, fiber optic and VSAT. Each RTU shall be connected to both the CFEs through a splitter, unless a RTU has a redundant communication channel.

5.7 RTU/SAS communication over IEC 60870-5-104

The CFE shall be provided with suitable interfaces for communication with the RTUs/ **SAS** over IEC 60870-5-104 protocol. One set of Router cum firewall for RTUs/**SAS** shall be provided between RTUs/**SAS** and CFE for RTUs communicating with control center on IEC60870-5-104 protocol as per the **Part-B Appendix-F**.

5.8 Networking Equipment

5.8.1 Firewall

Firewalls shall be provided as per BOQ. It is required that both internal and external type firewalls are supplied from different manufacturers and have different Country of Origin. The external firewalls includes firewall for RTU/ICCP and external DMZ. All firewalls shall be hardware box firewall as per the requirements mentioned in Appendix- H. Vendor has to keep all license updated throughout the contract period and provide the license validity till the completion of contract including AMC **(including extension if any).** Various desirable features of Firewalls are mentioned in **Section 9**.

All the data exchange from outside the control centre shall be routed through Firewall only.

The contractor shall provide a Network-based intrusion detection and prevention system coupled with the Firewall solutions to detect and prevent intrusion, worm, virus etc. Its main functions also include protecting the network from threats, such as denial of service (DoS) and unauthorized usage. It monitors the network for malicious activity or suspicious traffic by analyzing the protocol activity. This, in turn, makes the network intelligent and quickly discerns good traffic from bad traffic. Definition updates for virus, signatures, software patches etc. shall be done up to AMC period.

External Firewall (DMZ) shall support Multi-Factor Authentication (MFA) functionality also which shall be used for VPN and other purposes. MFA shall generate one-time password (OTP) and shall be available to the users via SMS, E-mail, through mobile application or dedicated token-based devices.

5.8.2 Anti-APT (Advanced Persistent Threat)

An advanced persistent threat (APT) is a covert cyber-attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period. The intention of an APT is to delete/damage or steal confidential data, cause a network outage, denial of service or infect systems with malware.

The changing nature of advanced persistent threats require dynamic protection solutions i.e., Anti-APT. Dynamic data protection identifies potential risks for data assets by monitoring and controlling assets in near real-time. Anti-APT detects and prevents targeted attacks. It enables detecting attacker presence on the network with maximum speed and recreating a full picture for thorough investigation.

Anti-APT shall be connected in external DMZ and shall work with external Firewall.

5.8.3 Network Access Control (NAC)

Proposed Network access control (NAC) solution shall keep unauthorized users and devices out from of a SCADA network. Solution shall restrict access to only those devices that are authorized and compliant with security policies, meaning they have all the required security patches and anti-intrusion software and blocks access of endpoint devices that do not comply with security policies. This ensures that a virus cannot enter the network from a device that originates from outside of the network.

NAC solutions shall control the access to the networks through the following capabilities:

- Policy lifecycle management: Enforces policies for all operating scenarios.
- Profiling and visibility: Recognize and profiles users and their devices before malicious code can cause damage.
- Security posture check: Evaluates security-policy compliance by user type, device type, and operating system.
- Incidence response: Mitigates network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention.
- Bidirectional integration: Integrate with other security and network solutions through the open/RESTful API.

5.8.4 Local Area Network (LAN) and device interfaces

Servers, Storage, Security devices etc shall be connected through high bandwidth capacity (10 Gbps) and shall be connected on FO based local area network (LAN). Peripheral devices shall be connected to each other on a copper / FO based local area network (LAN) as per the architecture and design. Dual LAN is envisaged for the System at Main and backup Control Centres.

Different networks connected in same switch shall be segregated through VLAN. LAN switches shall be as per the features mentioned in **Appendix- H**. Minimum number of ports requirement is specified in **Appendix-H**, however, contractor shall consider more number of ports as per the design. Colour of the LAN cables must be specified for easy identification with different LAN networks.

5.8.5 Routers

Routers shall be capable for data exchange between Control Centers, RTUs, Remote VDUs over various communication media such as copper cable, PSTN /leased line, fiber optic cable, VSAT etc. Routers shall have the built-in firewall/security features as required. There shall be 50% spare ports. Router shall be provided with necessary license support till the completion of contract including AMC (including extension if any). Router shall have L3 ports and proper access list shall be defined. Required features of Routers are mentioned in **Section 9**.

5.8.6 Workstation Consoles

Workstation console shall consist of a workstation driving two LED monitors, a single keyboard and optical mouse. The user shall be able to switch the keyboard and mouse, as a unit, among all the monitors at a console seamlessly.

Workstation consoles shall be used by the dispatchers for control, monitoring and operation of power system. All workstation consoles shall support full-graphics displays.

Each workstation in the Control room shall be provided with two speakers for alarming as per **specifications**. In addition to the speakers, the Contractor shall provide all other interface hardware, such as cables and connectors as required.

5.8.6.1 Remote console –

The remote consoles are workstations of different type which are to installed outside the control room.

These will be connected either on LAN /extended LAN or through a wide band communication link through a router. The remote console shall primarily be used as interface for the SCADA user application and Data historian application. The remote console shall have access to all the displays, trends and reports available in the local Operator workstations for SCADA and Data historian.

The remote consoles are of different types as mentioned in Appendix-H.

a) Remote Console with Dual monitor

b) All-in-One workstations with CPU

c) Remote Consoles with 55" Monitor with CPU

Integrated Remote Consoles (All in One): The Integrated remote console shall be provided wherein the workstation is part of monitor structure/ frame.

5.8.6.2 Video Wall –

In addition to remote console, there will be video wall consoles as per Appendix-G with Wall/Floor mounted monitors.

For 55" wall mount video wall, CPU shall be accommodated between wall and screen.

All the supplied system shall be supplied with stands (Wall/Floor) as per the Employer/Owner requirements during DRS approval.The video walls are of different types as mentioned in Appendix-H.

a. 55" video wall with controller

b. 55" video wall (Wall/Floor)

The video wall shall primarily be used as interface for the SCADA user application and Data historian application. The video wall shall have access to all the displays, trends and reports available to the local operator workstations for SCADA and Data historian, and shall also be available for the video wall users.

5.9 Storage Devices

5.9.1 Storage Area Network (SAN) based storage

A Storage Area Network (SAN) based or any other specialized storage solution shall be provided which shall be sized adequately and be used for online storage and all online data backup. Historian shall be connected to the servers through dedicated Fiber optic or Ethernet Port as applicable. The historian system shall facilitate owner's Application data storage also in proposed SAN. The sizing of the same shall be suitably sized by the contractor to meet the specification requirements. There shall not be any single point failure i.e. there shall be zero down time with single element failure.

5.9.2 Network Attached Storage (NAS)

The NAS shall be a dedicated file storage that enables multiple users and heterogeneous client devices to retrieve data from centralized disk capacity. The NAS shall be sized to accommodate storage of all data files of servers and workstations.

5.9.3 Backup Appliance

Backup appliance is a type of data storage device / equipment that accumulates the backup software and hardware components within a single device. Dedicated back-up appliance shall be provisioned for the backup of various files, database, image backup etc. as per the functionality mentioned under **Appendix-H.** It should be possible to restore or recover any software/system at a selected time from backup system. It shall be sized appropriately to take backup of all the supplied system.

5.10 Processor Terminal (Laptop):

The processor terminal shall be a Laptop to facilitate portability. It shall be primarily used for configuration of LAN, routers, etc. No separate furniture is required for the processor terminal.

5.11 Server Management console system:

Management console system shall be provided. It will be a system connecting all consoles of network devices to a single system through a switch. A separate LAN scheme should be available for management console and it should not interact with any of the SCADA LAN. It should be possible to configure, change and access any network device through this system console. All associated hardware and software shall be provided by the contractor.

5.12 Printers

All printers shall be interfaced with dual inbuilt/internal Ethernet LAN. Except for output capabilities unique to any printer type (such as extended character sets or graphic print capabilities), there shall be no limitations on the use of any printer to perform the functions of any other printer.

5.13 Video Projection System (VPS)

The contractor shall provide a video projection system based on modular DLP (Digital Light Processing) based high resolution **Laser** based rear projection technology as per BoQ. The VPS will be used to project displays of SCADA/EMS system independently of workstation console monitors. All the operations envisaged from workstation console (dispatcher) shall be possible from the VPS also. The VPS shall also be able to display Video signals and other Laptop/Computer feeds (VGA, HDMI, DVI and DP).

For the above purpose, it shall be ensured to connect different sources through HDMI for at least five no. of sources apart from SCADA/EMS system.

The VPS shall enable users to display inputs from multiple sources/applications simultaneously in freely resizable and repositionable windows on entire display area to enable effective collaboration and faster decision making.

The Contractor shall supply all necessary hardware and software, including Display controller, modesty panel, Base stands for VPS (arrangement's in base stand to accommodate the controller (without external panel) with sliding facility for future maintenance point of view), multi-screen drivers, adapters and memory to seamlessly integrate the video projection system with the user interface requirements described in the specification.

The video projection systems shall be rear projection systems and shall be complete with all projection modules, base stand with requisite supporting structures, cooling system and cabling. Design & installation of the video projection systems shall be coordinated with the Owner during project implementation.

The VPS controller shall synchronize its time with the SCADA/EMS system. The supporting structures of VPS should also accommodate Controller and Time and Frequency Display System.

The Visual Display Unit / Rear Projection Modules shall have in-built redundancy in **Laser** and ensures redundancy at the light source colour. The Projector shall support a flicker free image on the wall.

Time and frequency display shall be suitably placed on customer's requirement on any side of the VPS. Sufficient facility/space should be available on top or side of VPS to fix System frequency, Time and Date modules which shall not affect any display on VPS screen

The VPS controller shall have SNTP clients for synchronizing its time with the SCADA/EMS system. The supporting structures of VPS should also accommodate Controller and Time and Frequency Display System. A panel matching with VPS panel shall be supplied for installation of VPS Controller as well as Time and Frequency Display System. The Visual Display Unit / Rear Projection Modules shall have in-built redundancy and ensures redundancy at the light source color. The Projector shall support aflicker free image on the wall. VPS shall provide sharing of on-screen content on remote displays.

VPS shall provide sharing of on-screen content on remote displays. Message Ticker facility shall be provided to display the user entered highlights.

Message Ticker facility shall be provided to display the user entered highlights. Sufficient facility/space should be available on top or side of VPS to fix System frequency, Time and Date modules which shall not affect any display on VPS screen. Side of the VPS shall be covered with border for aesthetic look. Type Test Reports shall be provided for VPS and accessories during engineering approvals. The Type Tests should have been carried out at nationally/internationally accredited labs.

5.13.1 Testing methodology for VPS

The testing methodology for VPS is as below-

From each batch/total BoQ quantity of VPS modules for each control center offered by the Contractor for Factory acceptance testing (FAT), the Employer shall select random configuration as sample(s) to be tested for each Model of equipment for acceptance. All required FAT tests as per approved FAT procedures, shall be performed.

The physical verification and/or random Power ON tests shall be carried out on 100% of the offered quantities as per the approved FAT procedure. In case, any of the selected samples fail, the failed sample is discarded for dispatch, and additional minimum 2 (two) samples of same make/model/type shall be selected randomly (from the offered lot) and tested.

In case any sample from the additional two samples also fails, the entire batch shall be rejected. However, the above requirement is tentative, the exact sampling criteria/methodology for FAT shall be finalized during Detail Engineering stage.

5.13.2 VPS Module

The requirements for each modular VPS wall are as follows: -

a) The VPS wall shall be a seamless rectangular array wall, formed using modules in straight or curved arrangement **up to 15** degrees. The screen shall not contain any holes, stitching, screws in the active viewing area.

b) The screens shall be capable of displaying full resolution of the source.

c) The configuration of the VPS wall (no. of cubes and size of each cube) is defined in the Bill of Quantity. The height of VPS above the ground level shall be decided during detailed engineering based on the layout of the control room and available clear height.

d) The VPS wall should be rugged in nature and shall be designed for 24X7 operational environments. Necessary cooling arrangement for VPS shall be provided with the VPS. The air-conditioned environment in the Control room shall be provided by the Owner.

e) The optimum brightness of VPS display shall be maintained throughout the contract period including VPS.

f) The VPS shall be designed to prevent dust ingress.

5.13.3 VPS wall Management Software

The VPS wall Management Software shall have the following features:

a) The management software shall be able to pre-configure various display layouts (arrangement of different windows) and access them at any time with a simple mouse click. The window can be of different size and could contain display from different applications/sources.

b) The management software shall enable the users to see the desktop of the VPS wall remotely on any Windows based PC connected with the Display Controller over the Ethernet and change the size and position of the various windows being shown.

c) The management software shall enable various operators to access the display wall from local keyboard and mouse of their Windows workstation connected with the VPS Controller over the LAN.

d) The management software shall be able to push the screen content of a Windows PC / workstation to be shown on the Display wall in scalable and moveable windows in real time environment. The Windows PC/workstation shall be connected to the local Display Controller over LAN.

e) The Wall Management software shall allow display of video/data windows inside other graphic windows and it should be possible to configure the video/data windows to always remain on top while the operator works on the windows below.

f) The wall management software shall support open APIs to enable system integrators to integrate it with their Software. These APIs shall be provided for SCADA/EMS system.

g) Universal interactive console (with mouse/touchpad, keyboard, controls etc.) shall be provided for managing all video walls from the same console/workstations placed in control room from the same console.

h) The management software shall provide the authentication feature for the operators such as through identity management software.

5.13.4 VPS diagnostics and maintenance

The Diagnostic software shall perform health monitoring that allows timely detection of faults and provide at least the following: -

a) Cube health
b) LED **source** age, expected life left
c) Monitoring of critical Cooling
d) Selected inputs and presence of sources on either input
e) Brightness level & adjustment

The VPS maintenance Software shall allow commands on wall level or cube level ora selection of cubes for at least the following: -

a) Switching the entire display wall or display cube or a selection of cubes ON or OFF.
b) Provide tool for adjustments to keep the wall picture uniform over time.
c) Users shall be provided option of manual or auto adjustment of color and brightness of the cube/wall.
d) Changing the active input (of the two present DVI inputs).
e) Fine tune color of each cube.
f) Setting all projection modules to a common brightness,
g) It shall provide a log, such that:
    - It records events
    - It can record status at given time intervals
    - It can be exported to excel/html
    - It shows internal patterns, etc.

The VPS must allow easy removal of the components for maintenance.
Sufficient facility should be available on top or side of VPS to fix System frequency, Time and Date modules which shall not affect any display on VPS screen.

In case of replacement of any module of VPS, the contractor shall ensure the matching of the colour with the modules installed.

5.14 Time Facility

To determine Universal Coordinated Time (UTC) source NAVIC based Time Facility (with fail back option to GPS) shall be provided for Control Centre computer system. The time receiver shall include propagation delay compensation and shall also include an offset to permit correction to local time. The GPS system shall be equipped with a controller and dual receiver.

The time receiver shall detect the loss of signal from the UTC source. A loss-of-signal shall be sent to the computer systems and used as a telemetry failure indication and result in an alarm in the SCADA system.

The NAVIC/GPS based time receiver unit shall have digital displays for viewing UTC Day of the year, time frequency and time block display. The frequency display shall have suitable interface with the SCADA system such that any selected power system frequency measurands in the SCADA system can be assigned to it. Local frequency shall be captured and displayed in SCADA for the operator.

It shall be possible to do measurement of local frequency from Raw supply with resolution +/-0.001 Hz. The specifications for NAVIC/GPS based time receiver and the digital displays are given in **Appendix- H of Part-B**. NAVIC/GPS time receiver shall provide time sync to all SCADA/EMS applications. All required interface in this regard shall be included in the scope of supply.

All required interface in this regard shall be included in the scope of supply.

There should be a provision to capture local RAW power frequency and integrated with SCADA system to display in real-time and archival of the same.

Both the NAVIC/GPS based time receivers shall be configured in redundant mode and all system will synchronize time from both the sources.

5.15 Power Supply for Control Centre equipment

The computer system should be suitable for operation with single-phase, 230 +10% Vac, 50 + 5% Hz power supply. The UPS system comprises of redundant UPS operating in parallel and shall be used to ensure uninterrupted & regulated power supply to the computer systems. The Contractor shall provide additional fuses, switches and surge protection, if necessary to protect the computer system hardware. All cables supply, laying & their termination between UPS panel & computer system shall be in the scope of contractor.

5.16 Furniture

The control room furniture, from reputed make, shall conform to high standard of engineering as mentioned in the document, meeting the specified codes, standards, and designs. It shall be capable of performing 24X7 operations under the specified environmental condition in compliance with control room ergonomic norms i.e., ISO 11064. However, the specific design, finish and color of all furniture shall be subject to Employer/Owner's approval.

General requirement for Workstation Desk (both type)

I. **Structure**

a) Made of heavy duty extruded vertical and horizontal aluminum profiles of 6005 grade duly powder coated.

II. **Tabletop**

The material of the working surface shall be minimum 25 mm thick MDF with High Pressure ANSI/NEMA LD3 certified scratch-resistant laminate and having balancing laminate of minimum 0.5 mm thickness other side. The proposed desk life cycle shall be assessed for environmental impacts associated with all the stages of a product's life for cradle to grave analysis.

III. **Slat Wall**

Slat wall shall be made of approximately 2mm thick extruded aluminum (aluminum alloy).

IV. **Front Edge**

UL/ Intertek/NABL certified Lab audit certified design feature on front modular Polyurethane (PU) Edge. High density Poly Urethane Foam molded on industrial grade aluminum core to form minimum 50mm deep tapered edge to be installed on worktop.

V. **Shutters & Side Legs**

Front and back shutters shall be of 18 mm Laminated MDF Board with premium finish. The side leg shall be of 25mm of the same finish.

VI. **Hardware**

All bolts shall be of SS material to avoid rust due to environment. Remaining hardware shall be Nickel Plated MS.

VII. Table shall have been provided with sufficient number of power sockets, LAN ports, door-lights, sliding trolley for CPU, soft-door closure etc. Number of sliding trollies, LAN port and power sockets may be provided as per the owner additional requirement.

a) Workstation Desk: Motorized

Each workstation shall be provided with a suitable desk as follows:

a) Sectional frame suitably clad with hardwood or hard wearing material.
b) Desktops of a durable, scratch resistant, non-reflecting finish of suitable thickness.
c) Proper Channels for Power, LAN and Telephone cabling with 100% spare capacity i.e., integrated cable management system shall be in place.
d) Adequate space shall be provided on the desktop for the writing area, to accommodate the operator workstation, mouse, telephone and other miscellaneous items.
e) Drawers, shelves, and miscellaneous fittings.
f) Access shall be allowed for maintenance to equipment mounted on or in the desk. Pull out Drawer, Doors or removable panels shall be provided for this purpose.
g) Adjustable (height) desks (sit-and-stand with step-less automatic height adjustment).
h) Independent electronic powered height adjustment of monitors platform and workspace.
i) Table shall have been provided with sufficient number of power sockets, LAN ports, door-lights, sliding trolley for CPU, soft-door closure etc. Number of sliding trollies, LAN port and power sockets may be provided as per the owner additional requirement.

j) Monitor tilt variation with motorized height/tilt/depth adjustment. Monitor screens' tilt shall be adjusted with electrical drive at desired angle, depth & curvilinear arrangement of screens depending on the operator's ease of working. All the monitor screens must have synchronized tilting with 0 to 60^{o} from vertical plane by single control, customizable.

k) Programmable touch screen controls for operator desk movements with auto-save PRESET options related to desk movements/position. Embedded screen option can be explored.

l) The programmable touch screen shall have at least 10 automatic preset to define the desk configuration as per individual operator's requirement.

m) To ensure hassle free ergonomic operations/adjustments and durability of the product, the desk shall have **UL/Intertek /NABL certified Lab** audit certified feature on all mechanisms of desk.

n) All bolts shall be of SS material to avoid rust due to environment.

b) Workstation Desk: Normal / U-Type

Each workstation shall be provided with a suitable desk as follows:

a) Sectional frame suitably clad with hardwood or hard wearing material.

b) Desktops of a durable, scratch resistant, non-reflecting finish of suitable thickness.

c) Proper Channels for Power, LAN and Telephone cabling with 100% spare capacity i.e. integrated cable management system shall be in place.

d) Adequate space shall be provided on the desktop for the writing area, to accommodate the operator workstation, mouse, telephone fand other miscellaneous items.

e) Drawers, shelves and miscellaneous fittings.

f) Access shall be allowed for maintenance to equipment mounted on or in the desk. Pull out Drawer, Doors or removable panels shall be provided for this purpose.

g) Table shall have been provided with sufficient number of power sockets, LAN ports, door-lights, sliding trolley for CPU, soft-door closure etc. Number of sliding trollies, LAN port and power sockets may be provided as per the owner additional requirement.

h) All bolts shall be of SS material to avoid rust due to environment.

c) Chairs

- Two chairs shall be provided at each workstation.
- The chair shall be of high-backed design with arm rests, covered in durable woven material.
- The chairs shall be of good quality and suitable for continuous use without discomfort.
- Pneumatic Seat height and back angle adjustments shall be provided, capable of easy operation.

d) Furniture for Printers

Furniture table for printer shall also be provided which shall have pre-fitted power sockets, LAN ports etc.

Furniture/Fixtures for all other items which are not mounted in the racks shall also be provided by supplier.

The contractor shall provide the workstation desk, its chairs and printer table at same rate to owner whenever required during entire contract period.

5.17 Environmental Conditions

Equipment located in the computer/ control room shall operate over an ambient temperature range of 16 deg. cel. to 30 deg. cel., with a maximum rate of change of 5 deg. cel. per hour. Relative humidity will range from 20% to 80% non-condensing. Further, all Hardware to be supplied under the project shall be RoHS complaint (Restriction of Hazardous Substance) in Electrical & Electronics Equipment.

Environmental parameters such as temperature, humidity, etc. from server, VPS and server room shall be provided to the operator. Record of the same shall also be maintained and on requirement basis same can be extracted.

5.18 Acoustic Noise Level

The noise level of any equipment located in the server room shall not exceed 60 dbA measurements at three feet from the enclosure. The noise level of equipment located outside the server room shall not exceed 50 dBA three feet from the enclosure. Sound-deadening enclosures shall be provided where necessary to meet these requirements.

5.18.0 General Construction Requirements

The enclosures/panels, used for mounting or placement of equipment, shall be constructed in accordance with the following requirements.

5.18.1 Panels

Contractor shall provide 'Smart Rack Solution' for housing server and network equipment. This should be as per the latest industry standard/available in market.

In case the equipment is mounted in panel type of enclosures, then such enclosures shall be finished inside and out. All cabinet metal shall be thoroughly cleaned and sanded to obtain a clean, smooth finish. All surfaces shall be treated to resist rust and to form a bond between the metal and the paint.

Moving assemblies within the enclosure, such as swing frames or extension slides, shall be designed such that full movement of the assembly is possible without bending or distortion of the enclosure or the moving assembly. Enclosures shall not require fastening to the floor to preclude tipping of the enclosure when the moving assembly is extended. No cables shall be visible, all cables shall be properly clamped, and all entries shall be properly sealed to prevent access by rodents.

Cooling air shall be drawn from the conditioned air within the room. Ducted or directed cooling air to the enclosures will not be supplied by Owner.

All wiring shall use copper conductors. Conductors in multi core cables shall be individually color coded.

Wiring within the enclosures shall be neatly arranged and securely fastened to the enclosure by non-conductive fasteners. 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 ofthe wire.

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.

The panel shall have double door on both sides.

The finish colors of all enclosures/panels shall be finalized during detailed engineering. The rack shall be provided with trays for mounting routers, KVM switches, NIPS devices etc.

Additional Scope for ERLDC Only: - The Smart Rack Solution design shall also include provision of intelligent Power distribution units (iPDUs) with inbuilt display at the designated Server / Switch Racks. iPDU is required for monitoring of current, power distribution, etc. of each equipment such as server, storage, switch etc. installed in smart rack. The data measured by iPDU shall be integrated to the local console and SCADA system. The necessary hardware and software required for integration of iPDU data with console as well as SCADA system shall be provided by the contractor. The iPDU shall be sensor-capable (Humidity & Temperature) shall allow thresholds to be set for sending automatic alerts when the inlet temperature of IT devices approaches the vendor-specified maximum to prevent servers and other devices from shutting down or failing due to overheating.

5.18.2 KVM

The contractor shall supply IP based KVM system as per the technical specification. All the Servers shall be connected to KVM system and shall be accessible through IP in KVM system. Proposed KVM over IP (KVMoIP) system shall be connected to switches envisaged for server Management console system**.** Through this KVM over IP (KVMoIP) connection, users shall access and control servers simultaneously from centrally.

5.18.3 Enclosure Grounding:

A safety ground in accordance with Indian standards shall be provided within each enclosure and shall connect to the ground (green) wire of the ac power input. All necessary and required Earthing shall be provided and executed by the vendor. Earthing shall be provided by Owner. Connection to Panel shall be provided by contractor.

5.18.3 Interconnections

All signal cabling between component units of the computer systems shall be supplied by the Contractor. Plug-type connectors with captive fasteners shall be used for all signal interconnections. The connectors shall be polarized to prevent improper assembly. Both ends of each interconnection cable shall be marked (preferably with cable feruling) with the cable number and the identifying number and location of each of the cable's terminations. Each cable shall be continuous between components, no intermediate splices or connectors shall be used. Terminations shall be entirely within the enclosure.

5.19 Centralized Keyboard & Mouse Control Solution (CKMC)

The intent of Centralized Keyboard & Mouse Control Solution (CKMC) is to facilitate Real Time Grid Operators to access multiple systems including SCADA, WAMS, IT PC, etc. through single set of Smart Keyboard and Mouse. It shall facilitate Grid Operators with flexible and full access & control of Computer Systems, Display Systems (Video Projection System (VPS), Video Wall, PC Display Units etc.) and Peripheral Controls installed in Control Room. Contractor shall provide complete solution considering the work requirement of the owners.

The CKMC system shall establish modern computer and control system to permit operators to access and control any and all computer and Display Systems directly from their workplaces, consisting of all, any or a combination of:

- CKMC Management System (Hardware & Software)
- Smart Keyboard Console for Operator Interface (For Shift Operators)

The following functions shall be supported by CKMC system:

a) It shall be possible to control any and all sources from any workplace using a smart keyboard and mouse.
b) User shall be able to access, display and control any connected system from any workplace/desk, in accordance with his user rights.
c) User shall be able to quickly and easily assign sources to screens using the keyboard.
d) Single multifunctional smart console /keyboard per workplace shall be sufficient to switch between and control any and all systems, in accordance with individual user rights.
e) The proposed solution must include appropriate switching infrastructure to provide flexible switching of input sources at the workplace. The transmission must occur over a network independent from all existing systems and networks.
f) The transmission algorithms shall not require any of the customer's CPU power or network capacity. This should be completely secured and without interfacing with existing networks.
g) System latency shall be minimal. Operators shall not be able to notice any difference in performance while accessing local or remote systems.
h) It shall be possible to assign, display and manage user rights for individuals and user groups during ongoing operations.
i) The proposed solution must be designed for 24 X 7 Real Time operations and have option for full redundancy.
j) Provide all additional required Equipment/software and services necessary to ensure compatibility between new and existing equipment.
k) It shall be possible to access a single source through multiple CKMC system simultaneously with proper switching infrastructure.
l) Training of Owner's personnel.

5.20 Laptop for DTS

The standalone Laptop for DTS server shall facilitate portability of DTS server functionality. It shall have dual LAN interface. It shall be loaded with required Software to meet the functionality in standalone mode.

5.21 Provision of file transfer between OT and IT

Provision must be kept to for secure file and data exchange between IT and OT system and between other OT systems. Keeping all security measures and guideline. All necessary hardware & Software shall be provisioned by the contractor accordingly. File exchange shall be as per the owner convenience periodicity.

-----End of Section 5-----

Section 6

Configuration

Characteristics

Table of Contents

Section 6

6.0 Introduction

The ability of the SCADA/EMS systems to perform their specified tasks under normal conditions and under conditions of hardware and software failure is of paramount importance to owner/employer. This section presents requirements for monitoring and managing the hardware and software configurations of these systems.

6.1 Redundancy

The SCADA/EMS system envisages some functions as critical functions and others as non-critical functions as defined in Part-B of the specifications. Every critical function must be supported by sufficient hardware and software redundancy to ensure that no single hardware or software failure will interrupt the availability of the functions for a period exceeding the failover time.

The non-critical functions may not be provided with hardware and software redundancy.

The redundancy requirement for hardware of SCADA/EMS system at control centers shall be as follows: -

a) **LAN switches**: The System shall have dual LAN architecture. All LANs shall be configured as redundant. All equipment shall have dual LAN connectivity.

b) **Servers:** All the servers for critical applications shall be configured as redundant.

c) **Printers:** All Printers shall be non- redundant devices.

d) **Workstation Consoles: These shall be configured as non- redundant devices.**

e) **GPS based Time facility:** The time and frequency system shall be configured as a redundant device excluding display device as per BoQ.

f) **Routers:** Routers shall have physical redundancy as well as channel redundancy i.e. redundant channels of a remote destination shall be configured on different routers.

g) **VPS Equipment:** VPS equipment shall be configured as non-redundant device.

h) **RTU communication and channel interfaces:** Communication front end processors & its interface module shall be configured as redundant for both critical & non-critical communication channels (RTUs). RTU communication interface equipment such as modems shall be configured as redundant devices for critical RTUs & shall be configured as non-redundant devices for non-critical RTUs. RTU communication channels shall be switchable to the backup interface without processor failover.

i) **Communication interfaces with other control center computer systems:** The communication interfaces with other control center computer systems shall be configured as redundant.

j) **Communication interface with remote consoles:** The communication interfaces with remote console shall be configured as non-redundant devices.

6.2 Server and Peripheral Device States

A server group is one or more servers that perform a subset of SCADA/EMS or other application functions in either a primary/backup manner or distributed manner (where the on-line functions performed by the server group are distributed among multiple primary servers). For example, one server group may be configured to perform all SCADA and Scheduling Functions, while other server groups perform ICCP and PSA functions.

Server and device states shall identify the operating condition of each Server and peripheral device of SCADA/EMS systems and shall be used to determine the system's reaction when restart and failover operations take place. Server and device states shall be assigned by failover functions, restart actions, and by user command.

The system shall be designed in such a way that failover between main and standby server shall not result in any loss of data and shall take place without any delay. Also, synchronization operation between Master and Standby Server shall not result in failure of the servers.

6.2.1 Server States

Each Server shall be assigned to one of the following states: -

a) <u>Primary:</u> A primary Server performs any or all of the on-line functions described in this Specification.

b) <u>Backup</u>: A backup Server replaces a primary Server in the event of primary Server failure or upon user command. It shall communicate with the primary Server to maintain backup databases and monitor the state of the primary Server.

c) <u>Down:</u> A Server is down, when it is not communicating with the SCADA/EMS system and is not capable of participating in any system activity.

Note: In case of a replication/synchronization operation between Master and Standby Server which involves passing-on of updated partitions of information from Master-Server to Standby-Server, any failover operation during this replication/ synchronization period shall not result in failure of both servers.

The system shall be designed in such a way that the Standby Server shall take the Master role without any delay and without any loss of data in real-time. During server failover/changeover, no data loss and data jumping should occur on the trend. Further, during failover/changeover, no external script may be required to take care of data jump/garbage values etc.

6.2.2 Peripheral Device States

Each peripheral device shall be assigned to one of the following states:-

a) Primary: The primary peripheral device is logically attached to a primary Server or primary Server group. If the primary Server or primary Server group fails and its functions are reassigned to a backup Server or backup Server group, the peripheral device shall follow the reassigned functions.

b) Backup: A backup peripheral device is used to replace a primary peripheral device in the event of primary peripheral device failure. It shall communicate with the primary Server or primary Server group to maintain its readiness to be assigned as a primary device.

c) Down: A down device cannot be accessed by the SCADA/EMS system.

6.2.3 Functional Redundancy

Every critical function must be supported by sufficient hardware redundancy to ensure that no single hardware and software failure will interrupt the availability of the functions for a period exceeding the failover time.

Replacement of faulty items of the system and its restoration shall not result in any loss of functionality or performance. The standby elements of redundant system shall be fully monitored at all times.

Non-critical functions are those that support maintenance and development of database, application software and training of users. No hardware redundancy is envisaged for these functions. However, as a minimum requirement bidder has to supply as per the technical specification.

6.3 Server and Device Interconnections

Redundant interconnections shall be provided among all Servers within a Server group, among all Server groups, and among all Servers (including Server groups) and all workstations located in control centre. The interconnections shall support Servers and peripheral devices data exchange over both the LANs. Recovery from a single LAN or any other interconnections failure shall not require any failover.

6.4 Backup Databases

The system shall maintain backup copies of all databases without requiring any manual intervention, so that system operations may continue in the event of Server, device, or software failure. The backup databases shall be updated with the current contents of the primary databases such that all changes to a primary database are reflected in the backup database **within 30 seconds** of the change. The backup databases shall be maintained in such a manner as to be protected from corruption due to Server and device failure. Backup databases shall be preserved for system input power disruptions of any duration. The information maintained in the backup databases shall include:-

a) Telemetered, calculated, and manually-entered values and their attributes, including quality codes, control inhibit state, and tag data.
b) Data and associated attributes maintained by the Information Storage and Retrieval function.
c) Alarm, event, and summary displays (such as off-normal, control inhibit, and alarm inhibit displays) or sufficient information to rebuild the displays in their entirety (including the time and date of the original data entries, not the time and date the display is newly created)
d) Application function execution, control, and adaptive parameters and input and output data, including power system analysis and scheduling save cases.

All Changes resulting from the addition or deletion of items in an existing database, structures and restructuring of databases shall be automatically backed up in the backup databases by the backup function.

6.5 Error Detection and Failure Determination

All Servers, devices, on-line functions, and maintenance functions in system shall be monitored for fatal and recoverable errors. All errors shall be recorded by the system for review by maintenance personnel. Each type of error (e.g., Server failure, memory access violation, device reply time-out, or message checksum error) shall be recorded separately with a date and time tag.

Failure monitoring logic shall be distributed within the computing network and shall detect all failures that affect the availability of network resources or services. Failure monitoring functions shall be independent of application function and user modes. The failure monitoring and error detection function shall preferably provide event notification for 3rd party products e.g., SNMP messages.

6.5.1 Server Errors

All fatal and recoverable errors of all Servers operating in the primary and backup states shall be detected and recorded by the SCADA/EMS system. Server failure shall be detected and annunciated to the user **within 10 seconds** of the failure.

6.5.2 Device Errors

All fatal and recoverable errors of all peripheral devices shall be detected and recorded. Each type of recoverable error shall be assigned a threshold by the programmer. Peripheral device (except printers) failure shall be detected and annunciated **within 10 seconds** of the failure.

6.5.3 Software Errors

Execution errors in on-line and maintenance functions that are not resolved by program logic internal to the function shall be considered as fatal software errors. Fatal software errors shall result either in termination of the function or shall be handled as a fatal Server error. The action to be performed shall be defined by the programmer 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 by the programmer.

On the occurrence of each fatal software error, Server and operating system error codes and messages shall be recorded in the SCADA/EMS system. This record should be available for 30 days.

6.6 Server Redundancy and Configuration management

When a failure of a primary Server in a redundant group is detected, the computer system shall invoke the appropriate server failure recovery actions. Failure recovery is the capability of automatically transferring the functions (failover) from primaryhardware resources to secondary hardware resources or restarting the server whena failure-monitoring function detects a failure. The failover shall be the preferred failure recovery approach and restart shall only be used when failover is not possible.

After an error threshold-induced automatic transfer, the former primary server shall remain in an inactive (down) state so that a post-mortem analysis can be performed.A manual restart shall be necessary to bring it to the active ready state.

After a transfer caused by a Server failure or power loss, the former primary server shall either reboot into the ready state automatically or wait for manual intervention, depending on Employer's/Owner configuration management set-up.

If all alternate Servers are unavailable when the operating Server fails, the system shall attempt to automatically restart operating Server a programmable number of times.

Failures of Servers operating in the backup states shall not initiate failover or restart actions. The SCADA/EMS system shall only change the state of failed processor to 'DOWN'.

When a failure of a primary Server in a non-redundant group is detected, the computer system shall invoke restart actions. Functions assigned to a failed Server in a non-redundant group may be lost until the failed Server is restored to service.

All Server failures shall be annunciated by alarms. The alarms shall identify the failed Server(s), all Server state changes, and the success or failure of any restart and failover operations. For any server crash, manual transfer or threshold-induced transfer a crash dump file shall be automatically generated for analysis using standard interactive support tools. All such system events and crash dump file shall be transferred to Historian subsystem automatically.

6.6.1 Server Failover

A failover (transfer of critical functions) to an alternate Server shall occur, as a minimum, under any one of the following situations:-

(a) Non-recoverable failure of a server performing a critical function.

(b) User request for a transfer of servers.

(c) Failure of a periodic function to execute on schedule.

In the event of server failover, the functions of the failed Server shall be restarted in a working/functioning Server. Immediately upon detection of a failure, the failed Server's state shall be changed to down state. All devices assigned to the failed Server shall be reassigned to its backup Server without any manual intervention.

The on-line functions of the failed Server, having execution periodicity less than or equal to 30 seconds, shall be assigned to its backup Server **within 30 seconds of the failure** except for Historian Server. **In case of failure of Historian server; the Historian data shall be stored in the SCADA/EMS system till the failover of Historian server is completed to avoid data loss**. This stored data shall be transferred to the Historian server automatically after restoration of Historian server.

The on-line functions of the failed Server, having execution periodicity greater than 30 seconds, which were in progress at the time of failover or were missed during the failover, shall be assigned to its backup Server **within 120 seconds**.

6.6.2 Restart

Restart involves the ability of any server to self-detect its non-recoverable errors and to attempt to restart the SCADA/EMS system functions.

The restart logic shall determine the desired state of the failed Server and the on-line function(s) to be initiated in this Server. The restart logic shall also preclude conflicts among Servers, such as assigning too few or too many Servers to the primary state and the erroneous duplication of functions in multiple Servers. All maintenance functions executing in the restarting Server shall be suspended to expedite the restart process.

Restart shall include initialization of the SCADA/EMS function(s) and internal parameters, updating of databases, establishing access to peripheral devices, and execution of the function(s). Databases may be updated from backup databases or from static initialization database copies stored on auxiliary memory depending on the nature of the restart. The use of the static initialization databases shall be restricted to user-invoked restarts. If insufficient peripheral devices are available to perform the on-line function(s), the restart logic shall generate an alarm requesting user intervention. Restart as described above shall be completed **within 30 seconds** except **for EMS server** which can be **120 seconds**. **Also, the cold restart of the devices (Firewall, Router, Switch etc.) shall be completed within 5 minutes.**

6.6.3 Server Start-Up

A Server start-up shall be performed when commanded by a user and when Server input power is interrupted and restored such that the operating environment of the Server is established prior to restarting the on-line functions. Establishment of the operating environment may include execution of self-diagnostics, reloading the operating system and system services, and connection to and verification of communications with all nodes on the control center computer system LAN. The server start up shall be completed **within 5 minutes** with all functions scheduled for execution.

6.6.4 System Power-On-Start-Up

The SCADA/EMS system shall automatically restart itself when input power is interrupted and restored. System start-up shall include Server start up, initialization of all network devices, initialization of peripheral devices, initialization of all communications with data sources and other control centers, resumption of all SCADA/EMS functions and notifications to the users that startup has been completed. System power-on startup shall be completed within 5 (five) minutes or earlier.

6.6.5 Server Redundancy

All the critical functions shall reside on redundant servers. One of the redundant Servers shall normally be assigned to the backup state and it may also participate in on-line activity as a primary Server for some functions as per the design of the contractor. It is Owner/Employer's intent that each control centre computer system satisfies all of the performance requirements of this Specification with one Server of each Server group assigned to the backup or down state.

6.7 Peripheral Device Redundancy and Configuration Management

When failure of a redundant peripheral device is detected, the control center computer system shall automatically invoke the appropriate device failover actions so that on-line functions, which are using the failed device, are preserved. Failure ofa server's dependent device like auxiliary memory, if any, may result in server failover.

When failure of a non-redundant device is detected, the SCADA/EMS system shall not invoke server failover or server restart actions. On-line functions using a failed, non-redundant device may be lost until the failed device is restored to service.
All device failures shall be annunciated by alarms. The alarm text shall identify the failed device(s), all device state changes, and the success or failure of any device failover operations.

6.7.1 Device Failover

The device failover shall result in an orderly transfer of operations to a backup device in the event of failure of primary device. The device failover function may replace a failed device with an identical backup device or with a backup device that is different from the normal device.

Device failover actions shall be completed and the backup device shall be operating **within 30 seconds** of detection of the device failure.

6.7.2 Device Reinstatement

Except for communications with RTUs and the data links to other control center computer systems, failed devices shall be reinstated **by user command only**. If the control center computer system has failed any RTU, other data source, or the communication channel (including the modem/controller) connecting the system to the RTU or data source, communications with the RTU data source shall be retried at a periodicity specified by the programmer. When reliable communications are re- established, as determined by a programmer-adjustable number of consecutives retries (initially three), the RTU, data source or communication shall be automatically returned to Operation.

6.8 Configuration Management Displays

Each SCADA/EMS system shall include schematic and tabular displays for configuration management. The displays shall depict the state of each Server, peripheral device, and their interconnections, and include facilities for initiating user-commanded changes to the state and assignment of devices to Servers and user-commanded restarts, Server and device failover and Server start-ups. Displays to view and control the status of backup databases shall also be provided. Status of SCADA/EMS functions (Primary/ Backup) shall be displayed on the display.

6.9 Data Synchronization Between Main and Backup Control Centres

Both the Main and the Backup systems shall be operational during normal circumstances. Following should be salient feature:

RTU and ICCP Data:

- Both Main and Backup Control Centres shall get the data either on ICCP from associated Control centers or directly from RTUs as per designed architecture.
- Backup System can be updated from the Main by exception within 10 seconds.
- Both Main and Back up Control Centres will be in ACTIVE- ACTIVE Mode.

Historian Server:

- For Historian Server at Main Control Centre, source of Data will be from SCADA of Main Control Centre
- For Historian Server at Back Control Centre, source of Data will be from SCADA of Back Control Centre

- In case of failure of SCADA, user shall be able to synchronise data from other control centre for a defined/selected duration.

Data Base and Display:

- It shall be possible to synchronize databases used for development, display building and source code on daily basis automatically and manually both.
- The real-time databases (except the databases used for development, display building, historical data) at both the control centres shall be synchronized (integrity check) every 600 seconds.

The failover shall not be affecting the RTU data communication and they would continue reporting to the respective Control Centres and no data loss at Main and Backup Control Centres shall occur.

Both the Main and Backup Control Centre shall monitor each other's availability at least **every 120 seconds** by communicating to each other. An alarm shall be generated when a failure of the other control centre is detected. An SMS must be generated to predefined numbers in case of connectivity loss between main and backup control center.

In case of failure of the Main Control Centre, the Backup Control Centre shall takeover operations and functions. When Main Control Centre recovers from failure, Backup Control Centre shall update all data at Main Control Centre for the period it was down.

-----End of the Section6-----

Section 7

Inspection and Testing

Table of Contents

Section 7 Inspection and Testing

7.0 General requirements

All materials furnished and all work performed under this Contract shall be inspected and tested. Should any inspections or tests indicate that specific hardware, software, or documentation does not meet the specified requirements; the appropriate items shall be repaired, replaced, upgraded, or added by the Contractor as necessary to correct the noted deficiencies. After correction of deficiencies, all tests necessary to verify the effectiveness of the corrective action taken shall be repeated. Deliverables shall not be shipped until all required inspections and tests have been completed, all deficiencies have been corrected to employer's/owner's satisfaction and the hardware and software have been approved for shipment by the Employer/Owner.

7.1 Inspection

Employer/Owner representatives shall be allowed access to the Contractor's facilities during system manufacturing and testing and to any facility where hardware or software is being produced. Office facilities, equipment, and documentation necessary to complete all inspections and to verify that the SCADA/EMS system is being developed and maintained in accordance with the Specification shall be provided to Employer's/Owner's representatives by the Contractor.

Employer/Owner representatives shall be allowed to inspect the Contractor's hardware and software quality assurance standards, procedures, and records. Documents identified in the approved software quality assurance plan (defined in Part-A Section 3) will be inspected to verify that the Contractor has performed the required quality assurance activities.

The inspection rights described above shall not apply to subcontractors supplying standard computer hardware, peripheral equipment, and third-party software products. The inspection rights shall apply to subcontractors developing new software for inclusion in the SCADA/EMS system and to sub-system suppliers. Generally, equipment items shall be inspected and tested as part of the hardware integration demonstration described in coming sub sections, and third-party software products shall be tested as part of the functional performance test described in coming sub section.

7.1.1 Inspection Certificate

The Contractor shall give the Employer/Owner Inspector 14 days written notice of any material being ready for testing in India and six weeks for outside India. Such tests shall be to the Contractor's account except for the expenses of the Employer/Owner. The Employer/Owner Inspector, unless witnessing of the test is waived, will attend such tests on the scheduled date for which employer/owner Inspector has been so notified or on a mutually agreed alternative date.

The employer/owner Inspector shall, within 14 days from the date of inspection as defined herein, give notice in writing to the Contractor of any objection to any drawings and all or any equipment and workmanship which in his opinion is not in accordance with the Contract. The Contractor shall give due consideration to such objections and shall make the modifications that may be necessary to meet said objections.

When the factory tests have been completed at the Contractor's or Subcontractor's works, the employer/Owner Inspector shall issue a certificate to this effect within 14 days after completion of tests but if the tests are not witnessed by the employer/ Owner Inspector, the certificate shall be issued within 14 days of receipt of the Contractor’s Test Certificate by the employer/ Owner Inspector. The completion of these tests or the issue of the certificates shall not bind employer/ Owner to accept the equipment should it, on further tests after erection, be found not to comply with the Contract.

In all cases where the Contract provides for tests, whether at the premises or works of the Contractor or of any Subcontractor, the Contractor except where otherwise specified shall provide free of charge items such as labor, materials, electricity, fuel, water stores, apparatus and instruments, as may be reasonably demanded by the employer/ Owner Inspector or his authorized representative to carry out effectively such tests of the equipment in accordance with the Contract and shall provide facilities to the employer/ Owner Inspector or his authorized representative to accomplish testing.

The inspection by employer/Owner and issue of Inspection Certificate thereon, shall in no way limit the liabilities and responsibilities of the Contractor in respect of the agreed Quality Assurance Program forming a part of the Contract.

The Contractor shall keep employer/ Owner informed in advance of the time of starting of the progress of manufacture of material in its various stages so that arrangements can be made for inspection.

Record of routine test reports shall be maintained by the Contractor at their works for periodic inspection by employer's/Owner’s representative.

Certificates of manufacturing tests shall be maintained by the Contractor and produced for verification as and when desired by employer/Owner. No material shall be dispatched from its point of manufacture until it has been satisfactorily inspected and tested. Testing shall always be carried out while the inspection may be waived off by employer/Owner in writing only.

However, such inspection by employer's/Owner’s representative(s) shall not relieve the Contractor from the responsibility for furnishing material, software, and equipment to conform to the requirements of the Contract; nor invalidate any claim which employer may make because of defective or unsatisfactory material, software or equipment.

7.2 Test Plan and Test Procedures

Test plans and Test procedures shall be provided by the Contractor for all tests to ensure that each factory and site test is comprehensive and verifies the proper performance of the SCADA/EMS elements under test. During the development of test plans and test procedures for the system, emphasis shall be placed on testing each conditional logic statement, checking error conditions, and documenting the simulation techniques used.

The test plans and test procedures shall be modular to allow individual test segments to be repeated as necessary. They shall be subject to Employer/Owner approval (see Part-A Section-3).

For SCADA/EMS system guidance from Indian standard IS 15953:2011 "SCADA System for Power System Applications" should be included for FAT & SAT procedure. "

7.2.1 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:-

(a) Test schedule on a day-by-day basis

(b) Responsibilities of Contractor and Employer/Owner personnel

(c) Record-keeping assignments, procedures, and forms

(d) Procedures for monitoring, correcting, and retesting variances

(e) Procedures for controlling and documenting all changes made to the hardware and software after the start of testing.

(f) Block diagrams of the hardware test configuration, the external communication channels, and any test or simulation hardware.

7.2.2 Test Procedures

The test procedures shall describe the individual tests segments and the steps comprising each segment, particularly the methods and processes to be followed. The test procedures shall include the following items:-

(a) Name of function to be tested

(b) References to the functional, design, user, and any other documents describing the function

(c) List of test segments to be performed and the purpose of each test segment

(d) Set-up conditions for each test segment, including descriptions of the test equipment

(e) Descriptions, listings, and instructions for test software tools and displays if any.

(f) Step-by-step descriptions of each test segment, including user actions for each test step

(g) Expected results for each test segment, including pass/fail criteria

(h) Descriptions of the techniques and scenarios to be used to simulate system field inputs and controlled equipment

(i) Copies of any certified test data to be used in lieu of testing.

7.3 Test Records

Complete records of all factory and field acceptance test results shall be maintained by the Contractor. The records shall be keyed to the test procedures. The following items shall be included in the test records: -

(a) Reference to appropriate test procedure

(b) Date of test

(c) Description of any test conditions, input data, or user actions differing from that described in the test procedure

(d) Test results for each test segment including a pass/fail indication

(e) Identification of Contractor's test engineer and employer's representative if any.

(f) Provision for comments by employer's representative

(g) Copies of any variance reports generated

(h) Copies of reports, display copies, and any other hardcopy generated as part of the test.

7.3.1 Reporting Variances

Starting from the dry run test period, a variance report shall be prepared by Contractor personnel each time a deviation from the requirements of this Specification is detected in areas such as system functions, design parameters, performance, documentation, test plans, and test procedures. The report shall include a complete description of the variance, including:

(a) Sequential identifying number assigned to the variance

(b) Date and time the variance was detected

(c) Appropriate references to the test procedures and this Specification

(d) Description of test conditions at the time the variance was detected

(e) Identification of Contractor and employer/Owner representatives

(f) Estimated date and time when variance is expected to be fixed

(g) Description of the corrective actions taken (to be completed as part of the variance resolution process)

(h) Dated signature lines for the employer/Owner and Contractor representatives to signify reporting and correction of the variance.

Each variance shall be assigned to one of three classes defining the action to be taken to resolve the variance: -

(a) Class 1: Testing will immediately stop and the Contractor will evaluate and correct the variance before testing is resumed.

(b) Class 2: Testing will continue and the variance will be evaluated and corrected by the Contractor at the end of the current session but prior to further testing.

(c) Class 3: Testing will continue and the variance will be evaluated and corrected at a mutually agreed upon time.

The class shall be assigned by the Contractor with Employer/Owner approval.

Variance reports shall be available to employer for review and comment at all times and shall be submitted by the Contractor to Employer/Owner at the start of the availability test. The Contractor shall maintain and periodically distribute a variance summary that lists for each variance the report number, a brief description of the variance, its class, and its current status (open or resolved). A variance summary shall also be submitted with the progress report.

7.3.2 Resolution of Variances

All actions taken to correct variances shall be documented on the variance report by the Contractor. Sufficient information shall be provided to enable Employer/ Owner representative to determine the need for and extent of retesting, the need for testing interactions of the correction with any previously tested hardware or software, and the need for updating appropriate documentation. A variance shall be deemed resolved after retesting has been performed to the satisfaction of Employer/Owner and the Contractor and Employer/Owner representatives have acknowledged correction of the variance on the variance report.

7.4 Test Initiation

The following conditions must be satisfied before starting any test (exclusive of inspections or demonstrations pursuant to Section 7.2):

a) All test plans and procedures for the test shall be approved by Employer/ Owner.

b) All hardware and software engineering design change orders shall be incorporated into the system under test.

c) All relevant documentation including drawings, lists of deliverables, and software functional and design documents, and user manuals shall be approved by Employer/ Owner.

d) A complete regeneration of the software under test for which source code is being supplied shall be performed immediately prior to the start of factory testing.

e) All operating system parameters, files, and configuration information shall be saved to archive media so that the SCADA/EMS operating environment can be recreated starting with an un-initialized system. The existence and completeness of this data shall be demonstrated to Employer/Owner.

f) All database, display, and report definitions shall be saved to archive media so that the databases, displays, and reports can be recreated if necessary.

g) The image backup of all applications of SCADA/EMS system shall be taken on the archive media so that SCADA/EMS system software can be regenerated if necessary.

h) A complete dry run of each factory test (excluding the integrated system test) shall be conducted by the Contractor using the approved test plans and test procedures. Written certification that the dry run has been successfully completed shall be provided to Employer/Owner at least one week prior to the start of each factory test. At Employer/Owner option, Employer/Owner representatives will witness and participate in the dry run of any test.

i) SHA256 checksum of all Software binaries cleared for dispatch after testing shall be generated, recorded and submitted to Employer/Owner.

7.5 Test Completion

A test shall be deemed to be successfully completed only when:

a) All variances have been resolved to the satisfaction of Owner

b) All test records have been transmitted to Owner

c) Owner acknowledges, in writing, successful completion of the test.

7.6 Test Suspension

Any time Employer/Owner representatives can decide on the quantity/severity of variances that warrants suspension of any or entire testing, the test shall be halted, remedial work shall be performed by the Contractor and the Complete Test shall be repeated.

The repeat of test shall be scheduled for a date and time agreed upon by both the Contractor and Employer/Owner. Also, the class of variance can be decided or altered by the Employer/Owner based on the functional requirement and intent of the technical specifications.

Upon completion of above criteria, dispatch clearance will be accorded by the Employer/Owner.

7.7 Factory Acceptance Test (FAT) Requirements

The Hardware and Software as required to conduct functionality and performance testing of shall be staged and configured to carry out the FAT.

The Contractor is responsible for conducting all factory tests. Employer will witness all tests and will perform selected test procedures. Knowledgeable Contractor personnel shall be present at all times to assist employer representatives with factory testing as needed.

Employer will not accept un-witnessed test results of any hardware or software without previous written authorization. Each of the factory tests described below (i.e. Functional FAT, Integrated FAT, and the Simplified FAT) shall be carried out under factory tests. During FAT, serial number of products shall be noted.

Factory Acceptance Test (FAT) shall be conducted on full designed capacity of the supplied system i.e. sizing mentioned in specification and its expansion. Contractor shall make necessary arrangement to demonstrate the performance test.

Factory Acceptance Tests (FAT) shall be conducted in 3-stages as given below:

a) **Functional FAT** – complete functionality tests as per technical specifications and approved Functional FAT Procedure document shall be conducted on both Main and Back up control center of ERLDC. Functional FAT requirements are elaborated below at Section **7.7.1**.

b) **Integrated FAT** – Main and backup control centers of one RLDC and one SLDC along with Sub-LDC and 2 RTUs at each control center. Integrated FAT requirements specified below at **Section 7.7.2**.

c) **Simplified FAT** (Hardware Integration Test) – For balance SLDCs as specified below at **Section 7.7.3**.

The database, displays and the report formats developed by the contractor shall be demonstrated and verified by the Employer/Owner before factory testing.

All SCADA/EMS functions, inter-control centre communication as well as performance shall be tested and demonstrated, for Main & Backup CC configuration. The Employer/Owner will participate in and witness these tests.

Before commencement of FAT, the contractor shall also carry out testing of their IEC 60870-5-101 and 104 protocol implementations for successful integration by interfacing with existing RTUs. Before commencement of FAT, The contractor shall also carry out testing of their ICCP protocol implementation for successful integration by interfacing with existing Control Centers.

The database, displays and the report formats developed by the contractor for Main & Backup Control Centre shall be verified by the employer/ Owner before factory testing.

All hardware and software associated with all Main & Backup Control Centres shall be staged and completely tested with simulated data at the Contractor's facility as per above mentioned FAT tests.

The material inspection clearance certificate (MICC) for all hardware and software for all control center shall be issued only after successful completion of FAT tests as mentioned above.

7.7.1 Functional FAT

The functional FAT shall completely verify all features of the SCADA/EMS hardware and software for the Main and Backup Control center of ERLDC. As a minimum, the following tests shall be included in the functional FAT:-

- **Hardware Integration Test**: The hardware integration test shall confirm that the computer hardware conforms to this Specification and the Contractor-supplied hardware documentation. The hardware integration test shall be performed when the computer hardware has been installed in the Contractors factory.

The operation of each item shall be verified as an integral part of the system. Applicable hardware diagnostics shall be used to verify that each hardware component is completely operational and assembled into a configuration capable of supporting software integration and factory testing of the system. Equipment expansion capability shall also be verified during the hardware integration test.

- Inspection of all equipment for conformance to drawings/document and satisfactory construction and appearance
- Testing of the proper functioning of all software, including test caseswith normal and exception user-entered inputs and responses
- Simulation of local error and failure conditions
- Verification of all SCADA, EMS, CFE, Historian, NMS, Cyber Security functions **ect. and all features as specified in BoQ** and technical specifications and as per approved FAT procedure.
- Verification that ultimate expansion requirements are met.
- Verification of data link interfaces with other Control Centre systems
- Verification of RTU communication interfaces and data link interfaces with other control Centres computer systems. Simulation of RTU and data link communication errors and channel failures, including incorrect check codes and random channel noise bursts
- Testing of all user interface functions, including random tests to verifycorrect database linkages.
- Simulation of hardware failures and input power failures to verify thereaction of the system to server and device failure.
- Demonstration of all features of the database, display, and report generators and all other software maintenance features.
- Demonstration of the software utilities, libraries, and development tools.
- Verification that the computer system meets or exceeds Employer/Owner performance requirements.
- Verification of the accuracy of hardware and software documentation via random tests
- Testing of spare parts

7.7.2 Integrated FAT

The integrated system test shall verify the stability of the SCADA/EMS hardware and software after the functional performance test has been successfully completed on the selected RLDC/SLDC Main and backup control centers.

Integrated FAT shall be conducted with the following setup staged at Contractor's factory premises:

a) Main and Backup control centers of ERLDC

b) Main and backup control centers of any one SLDC along with its Sub-LDC (to be decided during Detail Engineering)

c) At least 2 RTUs for each control center mentioned above.

d) ICCP integration with these control centres and data exchange as per design and approval.

At least two RTUs for each protocol shall be connected with control centre and the remaining RTU shall be simulated in the factory test environment. The ICCP data exchange shall also be simulated in the factory test environment.

During the integrated system test, all SCADA/EMS functions shall run concurrently and all Contractor-supplied equipment shall operate for a continuous 100-hour period. The test procedure shall include periodic repetitions of the normal and peak loading scenarios defined in **Appendix-D of Part-B**. This minimum level of activity may be augmented, at the discretion of Employer/Owner, by other activities that represent normal day-to-day operation of the system as long as these activities are conducted in accordance with the training and documentation provided with the system.

These other activities may include, but shall not be limited to, verification of data integration between hierarchical control centers on various protocols such as ICCP/IEC 104, verification of failover reporting at downstream control centers and upstream control centers, database, display, and report modifications, software development activities, configuration changes (including user-commanded server and device failovers), and the execution of any function described in this Specification.

The integrated system test shall assure Employer/Owner that the computer system is free of improper interactions between software and hardware while the system is operating as an integrated unit. In case during the 100-hour period testing uncommanded functional restart or server or device fail occurs the test shall be extended by 24 hours each time such a fail over occurs. Further the test shall not be conducted with the failed device.

7.7.3 Simplified FAT

For balance SLDCs, which are not staged for Functional FAT or Integrated FAT, a simplified FAT shall be conducted with 2-3 control centers at a time. In this test, the basic functionalities, BOQ verifications, Data and Display verifications and power ON tests on random hardware items etc., shall be carried out. This test shall be witnessed by Employer and respective Owner SLDC representative.

7.7.4 FAT of miscellaneous items

The FAT methodology for balance miscellaneous hardware and software to be supplied under project which are not covered under section 7.7.1, 7.7.2 & 7.7.3 shall be decided during detail engineering.

7.8 Site Acceptance Tests (SAT) (also referred as Field Tests)

The Contractor's maintenance records shall be reviewed prior to Site Acceptance Testing (SAT) (also referred as Field Tests) to identify all hardware and software modified, repaired, or replaced between the completion of factory tests and the start of SAT. Interfaces to all communications circuits shall be established by the Contractor and the proper operation of these circuits shall be verified.

Site Acceptance Test (SAT) shall be conducted on full designed capacity of the supplied system i.e. sizing mentioned in specification and its expansion. Contractor shall make necessary arrangement to demonstrate the performance test.

For the purpose of interpreting the requirements for test plans, test procedures, test records, test initiation, and test completion, SAT shall be considered a single test accomplished for each computer system in three phases:

a) Site installation test

b) Pre-SAT (Pre-site performance test) and

c) SAT (Site Acceptance Test)

7.8.1 Site Installation Test (also referred as Field installation test)

The Site installation test shall provide verification that computer system is operationally equivalent to the system that successfully completed factory testing. The responsibility for the conduct of the Site installation test shall rest with the Contractor. Employer/ Respective RLDC/SLDC Owner will witness all tests and will perform all tests as per approved SAT procedures.

Knowledgeable Contractor representatives shall be present at all times to assist employer/Owner representatives with the testing. The Site installation test shall consist of the functional FAT test (Section 7.7.1) to confirm operation of basic functions such as data acquisition, user interface, and the support and utility functions. All hardware shall be tested by running diagnostics. The exact content of the site installation test shall be determined jointly by the Contractor and employer/Owner.

7.8.2 Pre-SAT (also referred as Pre-Field Performance Test)

After the Site installation test, the Contractor shall:-

(1) Verify the operation of RTU, data links and remote consoles

(2) Correct and update the database, reports, and displays

(3) Install and test employer/owner-developed software if any and

(4) Establish connectivity with SCADA/EMS system and another IT application provided by employer/owner. The Contractor shall be responsible for providing and installing corrections for all variances found during this period prior to the start of the field performance test.

7.8.3 Site Acceptance Test (SAT) (also referred as Field Performance Test)

After the completion of activities as per 7.8.2 clause, the Contractor shall conduct the SAT to verify those parts of the functional performance test (Section 7.7.1) that were not fully tested as part of the site installation test. All Class-3 Variances found during Integrated and Functional FAT tests and also All variances found during this SAT test period shall be fixed by the Contractor or otherwise resolved to employer's/Owner's satisfaction prior to the start of the **System Availability Test (SAVT).** The Site performance test shall concentrate on areas of SCADA/EMS operations that were simulated or only partially tested in the factory (e.g., system timing and loading while communicating with data links and system reaction to actual field measurements and field conditions). The validity of factory test results determined by calculation or extrapolation shall be examined. The Contractor shall be required to repeat selected portions of the Site installation test during the SAT if employer believes that previously tested functions have since been modified and are not operating in accordance with the Specification.

7.9 Unstructured Test

Provisions for unstructured testing by Employer/Owner personnel shall be provided during the FAT and or SAT, but before the starting of System Availability Test (SAVT). Methodology of unstructured testing is as given below:

Periods of unstructured testing shall be allocated to allow employer/owner representatives to verify proper operation of the SCADA/EMS **under conditions not specifically included in the approved test procedures but within the scope of Technical Specifications and/or approved test procedures**. Unstructured testing shall be conducted in compliance with the following conditions:-

(a) A minimum of 25 percent of the actual test period shall be reserved for unstructured test of the system by employer/owner representatives

(b) The Contractor's test representative shall be present and the Contractor's other technical staff members shall be available for consultation with employer/Owner personnel during unstructured test periods

(c) All simulation software, test cases, and other test facilities used during the structured portions of the factory/Site tests shall be made available for employer/Owner use during unstructured testing.

(d) Unstructured testing shall not begin prior to the start of the functional performance test at factory/site.

(e) Unstructured testing shall be allowed at employer/Owner discretion both at the end of a structured test segment and after completion of the functional performance test.

(f) Employer/Owner shall decide the need and timing of unstructured test during FAT and or SAT after completion of functional performance tests.

7.10 System Availability Test (SAVT)

After successful completion of SAT (i.e., field performance test), a 1000-hour system availability test (SAVT) shall be conducted on all supplied systems in an integrated and simultaneous manner under normal day-to-day operating conditions. The system under test shall include RLDC and all supplied SLDCs system (main and backup both) and RTUs under the respective RLDC/SLDC.

The test shall verify the reliability and integrity of the database, displays, report and all communication interfaces and, under these conditions, verify system availability for

99.9%. Further each server, device and RTUs, if applicable shall meet a minimum availability of 98% individually.

In case of RTUs, if applicable, downtime of individual RTUs are to be excluded from system availability calculations, however, minimum 50% of RTUs shall be reporting for test to continue**. In the event of repeated (not more than 3) unsuccessful re-runs of the availability test; Employer/Owner shall invoke the default provisions described in Volume-I, GCC, clause 23.2 of the specification**.

7.10.1 SAVT Test Responsibilities

Employer/ Owner will be responsible for conducting the system availability test (SAVT). The test shall consist of normal SCADA/EMS operations without special test equipment or procedures. Test records defined in the availability test plan and procedures will be maintained by employer/ Owner personnel. Employer/Owner will operate and maintain the system according to procedures described in the approved Contractor documentation.

SCADA/EMS maintenance on an on-call basis shall be provided by the Contractor during the availability test period. When on-site maintenance support is needed, qualified Contractor personnel shall arrive at the site within maximum four(4) hours of notification and shall keep employer/Owner fully informed of the progress in problem resolution. For availability purposes, this service response time and the associated on-site maintenance time shall be taken into account as defined in Sections 7.10.1.1 and 7.10.1.2.

The contractor shall maintain an inventory of spare parts, which may be required to achieve the specified availability. These spares shall be in addition to the mandatory spares. All spare parts used during the availability test shall be drawn from contractor's inventory.

During the SAVT test period, employer/Owner reserves the right to modify the databases, displays, reports, and application software. Such modifications will be described to the Contractor at least 48 hours in advance of implementation to allow their impact on the availability test to be assessed, except where such changes are necessary to maintain control of the power system.

7.10.1.1 Downtime

Downtime occurs whenever the criteria for successful operation defined in Section 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. For onsite response the delay in response time (more than four hours) shall be added to downtime.

7.10.1.2 Hold-Time

During the availability test, certain contingencies may occur that are beyond the control of employer/ Owner or the Contractor. These contingencies may prevent successful operation of the system but are not necessarily valid for the purpose of measuring SCADA/EMS availability. Such periods of unsuccessful operation may be declared "hold-time" by mutual agreement of employer/ Owner and the Contractor. Specific instances of hold-time contingencies are: -

a) **<u>Scheduled Shutdown</u>**: During scheduled shutdowns, or if an equipment failure occurs while its backup device is scheduled out- of-service, the resulting system outage shall be hold-time, provided that service can be restored according to Contractor-specified procedures **within 30 minutes**.

b) **<u>Power Interruption and Environmental Excursion</u>**: Loss of power or manual shutdown in the event of loss of environmental control shall be considered hold-time. If the system is operated during periods of power or environmental conditions beyond those specified, any resultant downtime shall also be considered hold-time.

c) **<u>Intermittent Failure</u>**: Periods during which an intermittent, recurring software or hardware failure is experienced will be considered hold-time, provided that the Contractor is engaged in remedial action and normal functions can be restored 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) **<u>Failure of employer/ Owner's Software</u>**: Time during which the system is down due to failure of software written and independently produced by employer/ Owner shall be considered hold-time. If a failure in such software cannot be overcome by Contractor- defined procedures, execution of the failed program will be suspended. Programs developed by employer/ Owner personnel under Contractor supervision are specifically excluded from this provision.

e) **<u>Service Response Time</u>**: A maximum **four (4) hours of hold time** will be allowed for the Contractor to respond to each call for maintenance support. The time between detection of a failure and the start of diagnostic procedures shall also be considered hold-time when performed by employer's/ Owner's personnel.

f) **<u>Corrected Design Defect</u>**: Hold-time may be declared by mutual agreement to ensure against similar future occurrences if a failure occurs due to a defect in system design for which the Contractor defines and implements corrective measures. In such a case, hold-time shall be allowed in increments of **120 hours** to allow verification of the corrective action.

7.10.2 SAVT Test Duration and Criteria for Acceptance

After the elapse of 1000 hours of cumulative test time, the availability shall be calculated considering the downtime recorded. Should availability fall short of specified percentage, the contractor may either (a) Continue the test by moving the starting time of the test forward and continuing the test until the consecutive hours have been accumulated and the specified availability has been achieved subject to **maximum of 75 days**, or (b) the contractor may restart the test for 1000 hours, however, more than two such restart shall not be allowed.

To establish that all failures have been satisfactorily repaired prior to the end of the SAVT, no downtime, intermittent (hold time) failures, or more than onecommanded fail over shall have occurred within 240 hours of the test's conclusion.

In the event of repeated unsuccessful reruns of the availability test, Employer/Owner may invoke the default provisions described in Volume I of the Specification. The successful completion of the availability test will lead to **Operational Acceptance** of the system.

7.11 Criteria for Successful Operation

The system shall be designed to meet the total system availability of 99.9%. That is, the ratio of total operational time minus downtime to total operational time shall be equal to or greater than 0.999. Total operational time shall not include the hold time. The system shall be considered available as long as all the critical functions defined under Section-2 of Part-B are available. Further each server and device and RTUs shall meet a minimum availability of 98% individually.

For ERLDC the operational acceptance shall be issued by respective owners and for balance SLDCs, the operational acceptance shall be issued by employer subject to fulfillment of criteria.

7.12 Contractor's Maintenance Responsibility till Operational Acceptance

During this period, the Contractor shall make available resident Project Manager, hardware & software specialists, who shall be available upon notification by the Employer/Owner about any problem(s) that may exist. The contractor's specialists shall be required to respond to the Employer/Owner's notification in line with the provisions of technical specifications. The contractor shall replace or repair all defective parts and shall have prime responsibility for keeping the system operational.

-----End of section7-----

Section 8

WEB AND SCHEDULING APPLICATIONS

Table of Contents

Section 8 Web and Scheduling Applications

8.0 Introduction

This section describes the functions to be performed by the Web and Scheduling applications being supplied by the Contractor.

The objective of web and scheduling Applications is to –

- Give web-based access to real time data, historical data, other data (such as Scheduling and Forecast Applications data) to authorized users
- Design interface of EMS/SCADA application to Outage scheduling application
- Integration of RLDC Schedule, Long term open access schedule, Short term open access schedule to SCADA/EMS system.
- Integrated data/information in web application server should be configurable with SCADA to update in SCADA database and network application (state estimator, outage schedules etc.).

These Applications are to be performed with due consideration for cyber security as per Information Security (ISO 27000). Only authenticated users shall be given Read/Write/Modify permissions based on their authority levels defined for different applications. There may be as many as 50 different categories of users for the same.

The IT services should generally comply the ISO 15000 standards for IT services management.

Design of system should meet high availability requirements and the web servers should be designed in cluster for load balancing However, in case of failure of one of the servers, all the clients shall automatically switch to the other server.

8.1 Scheduling Applications

8.1.1 Outage Scheduler (OS)

Outage Scheduler (OS) shall allow authorized users to enter, edit and maintain the outages of power system equipment. Enabling, the Control Centre to maintain records of all outage schedules that have been maintained/entered or edited by a user for devices recognized by Control Centre system.

Outage Schedular proposed should have capability to get integrated with EMS/Network Application databases for real time sequence of PSA studies. It shall be possible to distinguish (e.g., by colour coding or by adding a text) outage schedules of control centers on displays(for ex schedule entered at RLDC with the schedules received from SLDCs on displays).

Necessary features of OS are listed as follows:

i. Each Outage Schedule shall have unique identity. An outage schedule shall consist of following:

   a. Device identification
   b. Outage status,
   c. Start date and time
   d. End, date and time
   e. Note (reason for outage).
   f. Code issue time and date
   g. Code number of all LDCs involved.
   h. Type of outage (planned, forced, etc.). No restriction should bethere on number of "types of outages".

ii. It shall maintain all Outage Schedule revision history with the Schedule. Revision history shall keep track changes of all modifications with reason of modification and user name who modified it and the time of modification.

iii. It shall also monitor the actual outage against scheduled outage and report the deviation. It shall also categorize outages into planned outages or forced outages (tripping's/breakdowns).

iv. An outage shall contain one or more of the following devices in any combination: switching devices, AC and DC lines, transformers, phase- shifters, capacitors, reactors, and generating units.

v. Device identification as a minimum shall consist of the name of the station where the device is located and the name of the device.

vi. The Status of various devices shall be as per the practice followed by the Control Centre such as:

   a. Branches and Shunt Devices - In Service/Out of Service
   b. HVDC Facilities - Availability status and ratings for monopolar, bipolar, or back-to-back operation
   c. Generators -Availability status and ratings for possible operating modes.

vii. It shall be possible to enter schedules for up to one year in the future. Historical schedules shall be retained on-line for minimum one month from end of schedule and these schedules shall be transferred in data tables of Historian system daily and on demand for long term storage and reporting.

viii. Outage schedules for equipment modelled in the power system analysis and operations scheduling databases shall be used by other SCADA/EMS functions, such as Optimal Power Flow. For a specified future date and time, each SCADA/EMS function shall retrieve and use the status of the devices in the schedule that are appropriate to its needs. For example, Optimal PowerFlow shall retrieve the schedules for all devices.

ix. OS shall validate all entries to verify that the time span is valid, the device status is valid, and the new schedule does not conflict with any pre-existing and active schedule.

x. OS shall also check the device identification against the devices known to the system model and shall inform the user if the device identification is not found.

xi. The OS shall be able to accept outage schedule definitions from external source using standard API.The details of file shall be provided during detail engineering.

xii. The user shall be able to display the schedule for all devices at a specified date and time as well as display the schedule for a selected device over a specified time period. The user shall also be able to modify and delete any or all of the schedules maintained by OS.

xiii. User shall be able to import/export data from OS in a pre-defined format for a user-defined period.

xiv. User shall be able to run Power flow/study application on all the outages being given for the given time.

xv. As naming of elements (or tags) at RLDC may be different from that at SLDCs so mapping of names shall be provided such as; names importing from SCADA without any manual effort.

8.1.2 Load Forecast

Load Forecast provided under this project shall be Commercially Off the Shelf Product (COTS). The restricted quarter hourly megawatt demand of the system shall be forecasted for day ahead, week ahead by Load Forecast (LF).

The user shall be able to save the forecast results in any of **four output** save cases for future use. One of the save cases shall be designated the active load forecast for use by real time PSA functions. However, the study PSA functions shall be able to take any save case of Load forecast as input. In addition, the user shall be able to print and display selected results in both tabular and graphical forms showing restricted demands versus quarter hourly time instants.

LF shall support following method of load forecasting:

- Similar Day LF
- Profile based LF
- Average based LF
- Summation of LF received

Similar-day load forecasts shall be provided based on the quarter hourly restricted demand values actually computed and stored for each of up to seven different user-defined day types over the past twenty-five (25) months. It shall have capability to accept at least three weather parameters values. User shall have option to include weather input from Multiple sources. Also, users shall be able to forecast value based on areas defined within a state/region and final forecast shall be given after aggregating for area within state and states to give a regional forecast.

The user shall be able to enter three user-defined variables that describe predicted weather conditions for up to three predefined times of the load forecast day, such as temperature, relative humidity and precipitation level. The similar-day load forecast shall then search the past 25-month data for up to four days of the same day type as the load forecast day with weather condition variables that best match the predicted weather variables. LF shall allow the user to limit the search to all past days corresponding to:

(a) The load forecast day type

(b) One or more named months

(c) A time period specified by start and end date.

Each "best-match" load forecast shall include the mismatch errors between actual and predicted weather condition variables. The user shall be able to select and modify any of these forecasts to establish, for example, the active load forecast. This shall include the ability to scale only part of the forecast and the ability to adjust individual quarter hourly values to account for non-conforming load effects. The user shall be able to construct a multi-day forecast by defining the input data for each load forecast day prior to executing the similar-day load forecast.

LF shall automatically pickup forecasted weather parameters from a file (It may be an xml or text or MS Excel). Exact details of file shall be provided during detail engineering.

Profile based LF shall use the saved load profiles of the system. It shall be possible to save actual load of past days as load profiles. It shall support minimum 30 different profiles based on 15-minute load basis.

Average based LF, shall use actual load profiles of previous days. User shall enter dates/duration of time (from 2 days to 7 days) as input for LF. Based on these dates LF shall retrieve actual load on these dates and shall calculate quarterly hourly average of the loads during the specified dates/time period and this shall be Load Forecast for the selected future day.

LF application shall have web interface. It shall be possible to get load demand of stake holders through XML files using web services. LF shall sum up the values in the files (corresponding to same time period in each file) send by different stake holders to reach on the LF for future days. The interface shall also be provided for stake holders to enter their demand requirement using web for future days instead of using files. Then the LF shall be published on the web server for view by all stake holders as defined.

LF shall keep history of past twenty-five-month data. The storage shall be updated each day by replacing the oldest of the same day type with the current day actual load curve. The actual load for each quarter hour block stored shall be average of the quarter hour load corrected for 50 Hz frequency. While storing load in history it should also take into account load shed. It shall be possible to edit historical load data.

LF should have the feature of dynamic adjustment. Dynamic adjustments shall be based on the degree to which LF determines that the forecast does not match the actual restricted demand for two or more (Configurable) previous quarter hours. If average of mismatch for previous 8 (User configurable) quarter hours exceeds a User-adjustable threshold, LF shall determine and make the necessary adjustments to all future quarter hourly values of the current day's forecast automatically. The User shall have the ability to enable and disable dynamic adjustments to the current day's forecast.

Error statistics shall be maintained based on the difference between the restricted demand that is forecast six quarter hours in advance (user-adjustable) and the corresponding actual restricted demand when available. The statistics shall include the error in the restricted demand for each quarter hour for twenty-five months. It shall also calculate the mean and standard deviation of each error. The statistics for weather variable shall be maintained for twenty-five month and shall also calculate the mean and standard deviation of each error.

Reports based on Error Statistics as mentioned above may be generated. It shall also be show forecasted data in trend application of SCADA. Trends for Forecast Vs Actual comparison shall also be made available. Forecasted data shall be stored in Historian for all revisions and user shall be able to trend the same.

8.1.3 Integration with Scheduling Application (WBES)

The WBES application output data (quarter hourly schedules and five minute schedules of Generating Stations/plants and drawl schedules of constituents) for day a head shall be integrated with SCADA and network applications (State estimator etc.).

It shall have facility to integrate future schedule and trend for schedule, Forecast and Actual simultaneously in single trend window.

Units schedule shall be derived from Generating stations schedules by distributing the total station generation among units based on the unit availability by the Contractor application. Application shall be capable of adding unit values to reach at station values to compare scheduled versus actual generation of station values.

8.1.4 Integration and data exchange with Market Application

The application program Market Application (Owner's Existing application) output data shall be injection schedule at a node and Area, drawl/load schedule at a node on quarter hourly basis for future time period up to four months from current time. Contractor shall integrate these schedules with SCADA and network applications (e.g., State estimator). Application shall also have feature to manually enter injection schedule at a node and drawl/load schedule at a node.

8.1.5 Current Operating Plan (COP)

Current Operating Plan (COP) shall contain the active power system operation plan. COP shall contain information on quarter hourly basis for previous day, current day and one day in future. COP shall contain following information for above mentioned time period.

(a) Load Forecast

(b) Outage Schedules

(c) ABT Schedules (Plant schedules and Constituent Drawl schedules)

(d) STOA Schedules (Injection and drawl schedules)

8.2 Web System

Web System shall consist of all necessary hardware & software for Web Server, Data Replica Server and Web application. The SCADA/EMS system shall share the real time and historical data with Web server through Data Replica Server in secure manner. There shall be no data flow from Web system to SCADA/EMS servers. It shall get real time and historical data from SCADA/EMS System and share it with other stake holders. Data flow from SCADA/EMS servers to Web System will be one way i.e. SCADA/EMS servers will feed data to Web System and there will be no data flow from WEB System to SCADA/EMS servers.

It means that machines used to meet Web System requirement shall not be used for feeding data to SCADA/EMS servers. From operational requirement if transfer of data from DMZ Zone to SCADA zone will be required, separate database shall be created in DMZ from where data shall be read by SCADA Zone.

The data exchange and its publishing on WEB system (sharing data with other stakeholder) shall be done in secure manner ensuring the latest cyber security guideline from statuary authority.

8.2.1 Web Server

The Web Server shall be configured to provide the system information for public domain (default /Home Page View) and as well as user specific. The Web servers at the Main Control Centre are in active -active configuration and suitable load balancing shall be provided among the web servers.
However, in case of failure of one server, all the clients shall switch to the other server. The Web servers mentioned here are cluster of servers and shall be deployed to meet the requirements of external users for Power system real time and historical data and cyber security. Web server shall get the data (real time and historical) from Data Replica server and meet the requirements of web users (external users).
Web server in External DMZ shall be provided with host-based Intrusion detection system (HIDS). The HIDS will be installed on all the machines connected in the Web-server LAN. The NIPS shall be tightly integrated with the firewall.
Real time data on web server shall be refreshed every 20 second (configurable from 20 second to 1 minute). SCADA/EMS server fail over shall be transparent to the web servers.
Further, Tools shall be provided for maintaining the Web System, Web System configuration and customer support. Tools to assign displays, reports and data access

to user types shall be included. Tools to import SCADA/EMS Power System Applications (PSA) displays for web server shall be included. Latest protections against viruses shall be provided.

A display shall be provided to administrator accessibility of points to a user based on the Area, Company Station Name, Voltage level, generators, tie-lines, point type, point and any combination of these. This assignment to a user shall be applicable for both real time data and historical data access. e.g.: - User1 shall have access to only 1 display, user 2 can have access to 10 displays etc. depending on permission given by Administrator.

A display shall be provided which shall list all the analogs with details such as station name, voltage level, analog type etc. It shall be possible to filter and sort the data based on station name, voltage level and analog type. This display shall be accessible by only Supervisor/Administrator of SCADA/EMS System. This display shall be used to assign accessibility to a user based on the Area, Company and Station Name, Voltage level, generators, tie-lines, point type, point and any combination of these. This assignment to a user shall be applicable for both real time data and historical data access.

The email system shall be configured and integrated with mail server of the owner facility. Necessary applications to meet this functionality shall be provided. The contractor shall ensure appropriate sizing of web server, keeping in view, all the applications running/hosted on web server.

On log-in of web server by each external user/client a summary display shall be provided. This summary display shall guide user to navigate to different type of data e.g., real time data, historical data and reports. Depending on the selection, the user shall see the detail items accessible to him e.g., on selection of historical reports the user shall see reports accessible to him and on selection of analogs the user shall see analogs accessible to him with details such as station name, voltage level, analog type etc. It shall be possible to filter and sort the data based on station name, voltage level point type and its quality. The external client/users shall be able to download historical data by specifying the time window and selecting data points.

8.2.2 Data Replica Server

This server shall be used for staging all real time and Historical data to be served from Web Applications to external/web users so as to avoid exposure of SCADA/EMS system to external world. The server shall get snapshot real time data from

SCADA/EMS Server as it is available in real time and Historical data (data and reports) from Historian server and keep at least two months of historical data (at same sampling rate as stored in main historian). All data in Data replica server shall remain synchronized with the Historian placed in SCADA.

All user requests and application data requirement for Web server/application/ services shall be served from Data Replica server. Data Replica server shall be provided with latest host-based Intrusion detection system (HIDS).

8.2.3 Web Applications & Web Historian

The Web server at control centre is to function as source of information on Control Centre Power System. The web content shall be able to display on the latest version of commercially available general web browser such as Google Chrome, MS Edge, Firefox Mozilla, HTML5 or better, Safari etc., without installing any software on any device (Desktop/Laptop/Tab/Mobile) with appropriate display resolution and it should be accessed by diverse set of external users and full screen mode for application shall be available.

This application should be Mobile friendly application also. The web applications envisaged shall be made compatible for opening/ viewing on web browsers of any mobile devices. Such application should adhere to all the standard norms for technology, cyber security etc. as prevalent in the industry. The application provided shall be user friendly.

The access to Web server/site shall be controlled through two-factor authentication i.e. User ID and password to be maintained /granted by a system administrator and token generated through MFA application software.

Further, different displays, reports and data access shall be limited by user type (i.e., general user, shareholder, third party/business user). It shall be possible to define minimum 50 user types. The access mechanism shall identify and allow configuration of priority access to selected users. Also, source code of web page used for logging the users of web application shall be shared with the Employer/Owner.

The offered applications shall meet following requirements:

a) The web server/application shall provide access to any of the real time data and displays, for viewing by external clients/users. This access shall be controlled through User ID and password issued and maintained by a system administrator.

b) The Web-Portal shall provide the Access Control Management for Web and

Mobile devices. The user type and their access to the information/ views shall be finalized during detailed engineering. The access mechanism shall identify and allow configuration of priority access to selected users.

c) Sized to support 500 concurrent external clients/users for providing access to real-time and Historical data. There shall be no limitation on number of users. Each user shall be assigned to a user type.

d) External clients/users shall be connected to the web servers only. These users shall be denied direct access to the SCADA/EMS system.

e) Internal SCADA/EMS users shall not have any dependency on the availability of the application /server.

f) Data, Displays and Reports requested by External users/clients (access-based dashboards) shall be serviced by Web servers and if required it can be generated from Historian with in SCADA LAN.

g) The web Application/web-portal contents shall support Real Time Data Update such as Real-time Display of the grid parameters.

h) The web-portal/Web Applications provide the access of various reports to User such as Static Reports (Ex: Daily, Monthly, Yearly), Query Based Data /Historical Data for selected duration.

i) The Web-Portal shall provide the Access Control Management for Web and Mobile App.

j) There shall be Region Wise / user wise Dashboards for Data in web Application

k) There shall be ALARM / Events notifications for the contents of web portal/Web Application ex-: SCADA Event

l) The web-portal/Web Applications provide the access of various reports to User such as Static Reports (Ex: Daily, Monthly, Yearly), Query Based Data / Historical Data for selected duration.

m) Query System for generation of Historical Events recorded

n) For the purpose of transfer of data, displays and reports from the SCADA/EMS system to the Web System, Historian system shall initiate a session with the Data Replica server and any attempt to initiate a session by the Web system shall be terminated by the Firewall. Interface between Web system and SCADA/EMS and Historian System zone shall preclude the possibility of external clients defining new data, Report and Displays.

o) Display the Data (real Time) / Query Data in Trend Analysis with Export, RAW Data View options shall be there.

p) Real-time trend v/s past day trend of any data point shall be displayed in the web browser/mobile application.

q) Display the Substation's Data (real Time) in One-Line.

r) The information to be placed in public domain and restricted to internal users shall be segregated. The user authority level and their access to the information/ views shall be finalized during detailed engineering.

s) The Web application shall adhere to all latest cyber security guidelines issues by statuary authority from time-to-time.

t) The Web Publishing shall be interfaced / co-ordinated as per cyber security policy.

u) The Web Server shall provide access to any of the real-time data and displays/reports, for viewing and downloading by external clients/users. The access to each display/reports shall be definable on per user type basis. (i.e., general user, shareholder, third party/business user).It shall be possible to define up to 50 user types. SCADA/EMS System Administrator shall assign accessibility of any data and displays to any user types. All external users shall be provided with separate user login. Proper data validation and security check methods should be used before absorbing the data in the applications.

v) The Web System shall keep all Historian data on line minimum for last two months including current day, to enable downloading of selected Historian data by external users/clients. The data shall be updated in Web System as and when data is updated in Historian System. The above data points shall be definable on a per user type basis. The Web Server shall provide access to any of the Historian data and reports, for viewing and downloading by external clients/users. The access to each report shall be definable on per user type basis. SCADA/EMS Administrator shall assign accessibility of any data and reports to any user types.

w) The Web System shall keep all real time data on line, to enable viewing of selected Real-time data, both the values and a composite quality code of the selected Real-time data, both the values and a composite quality code of the points by external clients/users. The data shall be updated in Web System as points by external clients/users. The data shall be updated in Web System as and when data is updated in Historian System. The above data points shall be and when data is updated in Historian System. The above data points shall be definable on a per user type basis.

x) 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)

y) The web server shall enable downloading of selected Historian data. For the purpose of sizing, storage of two months Historian data for 100% of data points as specified in Appendix F shall be considered. The Historian data on Web System shall remain synchronized with the Historian system for above duration. The data shall be stored on Web System in any open system product e.g., my SQL. The external client/users shall be able to download the data by specifying the time window and selected data points on the web page. The above data values shall be definable on a per user type basis.

z) The web server shall store and make available for downloading and viewing selected real-time data, both the values and a composite quality code of the points for web users. For the purpose of sizing, data equal to 100% data points as specified in **Appendix-F** shall be considered. This data shall be made available in ODBL/OLE/XML/MySQL format in every minute (to be overwritten periodically). The users shall be able to download this file using web service. The above data points shall be definable on a per user type basis. It shall be possible to define up to 50 user types.

aa) The Web server shall also facilitate exchange of schedules and other information.

bb) 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).

cc) Web portal Interface with Multiple Database & External Application's Web page.

dd) A proper reporting tool should be provided for retrieval of data from Web Historian for reporting purpose. User shall be able to select the required Historian for reporting purpose. User shall be able to select the required parameters, duration etc and generate the report.

ee) User shall be able to plot various type of trends and access through web system which also includes comparison of present, future and historical values.

ff) Sound Notification shall be there in Web App/ Web-Portal on basis of Events.

8.2.4 E-mail and SMS interface for alarms:

It should have following functions:

- The Web server shall have necessary tools/utilities to automatically transmit text message contents for E-mail and SMS (short messaging service) to mobile phones through a Web based E-mail and SMS service provider. The message content of SMS shall be the same as the alarm generated by the system or a text string entered by a user.
- Email/SMS should be user configurable w.r.t the both individual point wise and alarm group wise.
- It shall be possible to create user defined email and SMS templates /ON-Demand SMS
- It shall be able to send Triggered Reports/Scheduled Reports to respected/ configured Email IDs
- It shall also be able to SMS (short message service) the summary report to defined mobile numbers.
- Email & SMS Integration with other Applications
- Provide a Provision to Configure Conditions basis Email & SMS.

SMS Interface

An SMS (short messaging service) interface application shall be provided by the contractor to meet SMS sending and configuring functionality envisaged under this section and other relevant sections of technical specification.
Contractor shall take services of SMS service provider and integrate the SMS interface with SMS service provider services to achieve SMS delivering functionality. Contractor shall take the services of SMS service provider for entire contract period (including extension of contract, if any). The contractor shall also provide services of SMS service provider for testing purposes during FAT, SAT etc. at its own cost.

The interface application shall be preferably hosted in web system to securely connect with SMS service provider services through use of encrypted APIs. However, the provided solution shall meet the cyber security related guidelines/policy envisaged in the technical specification.

Keeping cyber security aspects in design, SMS services from govt. agencies such as NIC etc. shall be preferred. As a minimum, following functionality shall be provided by contractor in the SMS interface at RLDC and SLDCs:

- User interface to configure various SMS alarms/alerts generated by SCADA/EMS system and associated IT monitoring and security systems like Firewall, NMS, Backup etc. The configuration application shall allow specifying categories of alarms/alerts to the designated pre-defined users/mobile numbers. Provision for Filtering alarm should be selectable from user interface without requiring any programing or scripts. The system should fetch user details of the recipients from the Active directory/other identity management system being provided.
- The configuration tool/interface should be only accessible after authentication with proper credentials. For this purpose, different type of users should be defined based on their access rights in the administration tool/interface.
- It shall be possible to pause the specific categories of alarms/alerts through controls provided on user interface with proper credentials.
- It shall have provisions to add/Modify/edit Categories of alarms/alerts details through suitable user interface with proper credentials. The alarms/alerts categories and parameter field details shall be finalised during detailed engineering. SMS should be configurable w.r.t the both individual point wise and alarm group wise.
- A minimum of adding 50 Users with pre-defined mobile numbers capability shall be provided in the solution. The user parameter field details shall be finalised during detail engineering.
- It shall have provisions to add/Modify/edit Users field details through suitable user interface with proper credentials.
- The solution shall be capable to take alarms/alerts generated by different applications and devices envisaged in the technical specification as mentioned in their relevant sections.
- Provision for conditional based SMS shall be there in SMS interface
- It shall also be able to SMS (short message service) the summary report to pre-defined mobile numbers. This functionality shall be configured based on the criticality of the power system element.
- An SMS must be generated to predefined numbers in case of connectivity loss between main and backup control center.
- The message content of SMS shall be the same as the alarm generated by the system or a text string entered by a user.
- It shall be possible to create user defined SMS templates / ON Demand SMS.
- SMS Interface application shall be configured as redundant in Main Control Centre and Backup Control Centre utilizing the same SMS service provider as envisaged in BoQ.

- Any unused quota of yearly SMS service provider (as envisaged in BoQ) shall be carry forward to subsequent years for utilization.
- There should be provision for viewing acknowledgement/delivery report logs for delivered SMS along with any delivery failure record.

The above functionalities shall be met preferably through web page interface developed in a user-friendly manner. The same interface shall also provide functionalities for performing administration/configuration related task.

The SMS interface should be accessible through commercially available Off-The-Shelf (COTS) web browsers. The contractor shall make desired/required changes/develop application in the interface APIs if SMS service provider is changed during entire project life cycle without any cost implication to owner.

- **Email Interface**

Contractor shall provide Email Interface to meet functionality for sending Email alarms/alerts envisaged under this section and other relevant sections of technical specification. Contractor shall also integrate this email interface with Owner's existing Email server (Existing Email server and ISP shall be provided by Owner).

The interface application shall be preferably hosted in web system to securely connect with utility existing email system so that the provided solution shall meet the cyber security related guidelines/policy envisaged in the technical specification. As a minimum, following functionality shall be provided by contractor in the Email interface at RLDC and SLDCs:

- User interface to configure various Email alarms/alerts generated by SCADA/EMS system and associated IT monitoring and security systems. The configuration application shall allow specifying categories of alarms/alerts to the designated pre-defined user/email addresses. The user details such as email addresses shall be fetched from the Active Directory/Identity Management System.
- The configuration tool/interface should be only accessible after authentication with proper credentials. For this purpose, different type of email users/email groups should be defined based on their access rights in the administration tool/interface. The users to whom the alerts shall be selectable based on the type of system, severity level of the alarms, location/site for which alert/event is being generated.
- It shall be possible to pause the specific categories of alarms/alerts through controls provided on user interface with proper credentials.

- It shall have provisions to add/Modify/edit Categories of alarms/alerts details through suitable user interface with proper credentials. The alarms/alerts categories and parameter field details shall be finalised during detail engineering. Email should be configurable w.r.t the both individual point wise and alarm group wise.
- A minimum of adding 50 Users with pre-defined email id capability shall be provided in the solution. The user parameter field details shall be finalised during detail engineering.
- It shall have provisions to add/Modify/edit Users field details through suitable user interface with proper credentials.
- The solution shall be capable to take alarms/alerts generated by different applications and devices envisaged in the technical specification as mentioned in their relevant sections.
- Provision for conditional based email shall be there in Email interface
- It shall also be able to send the summary report to pre-defined Email ids. This functionality shall be configured based on the criticality of the power system element.
- An Email must be generated to predefined Email addresses in case of connectivity loss between main and backup control center.
- The message content of Email shall be the same as the alarm generated by the system or a text string entered by a user.
- It shall be possible to create user defined Email templates / ON Demand Email.
- It shall be able to send Triggered Reports / Scheduled Reports to respected/ configured Email IDs to other domains also.
- Email Interface application shall be configured as redundant in Main Control Centre and Backup Control Centre utilizing the utility email servers. No dedicated email servers/ applications are envisaged with this specification.
- There should be provision for viewing acknowledgement/delivery report logs for delivered Email along with any delivery failure record.

The Email interface shall be configured and integrated with mail servers of the owner's facility. Necessary applications to meet this functionality shall be provided by contractor. In addition, administration tools to manage the Email interface application and for various configuration by contractor shall be provided through secure web access.
The contractor shall also provide any addition item/components (not envisaged in the specification) as required to meet the above functional requirement of SMS and Email without any cost implication to employer/owner.
A tentative architecture for SMS/Email interface functionalities is depicted below, the detailed architecture shall be finalised during engineering with due consideration to cyber security policy and guidelines mentioned in the specifications. For example,

Contractor may provision Alarms DB (as depicted below) in Data replica server to meet the above functionalities:

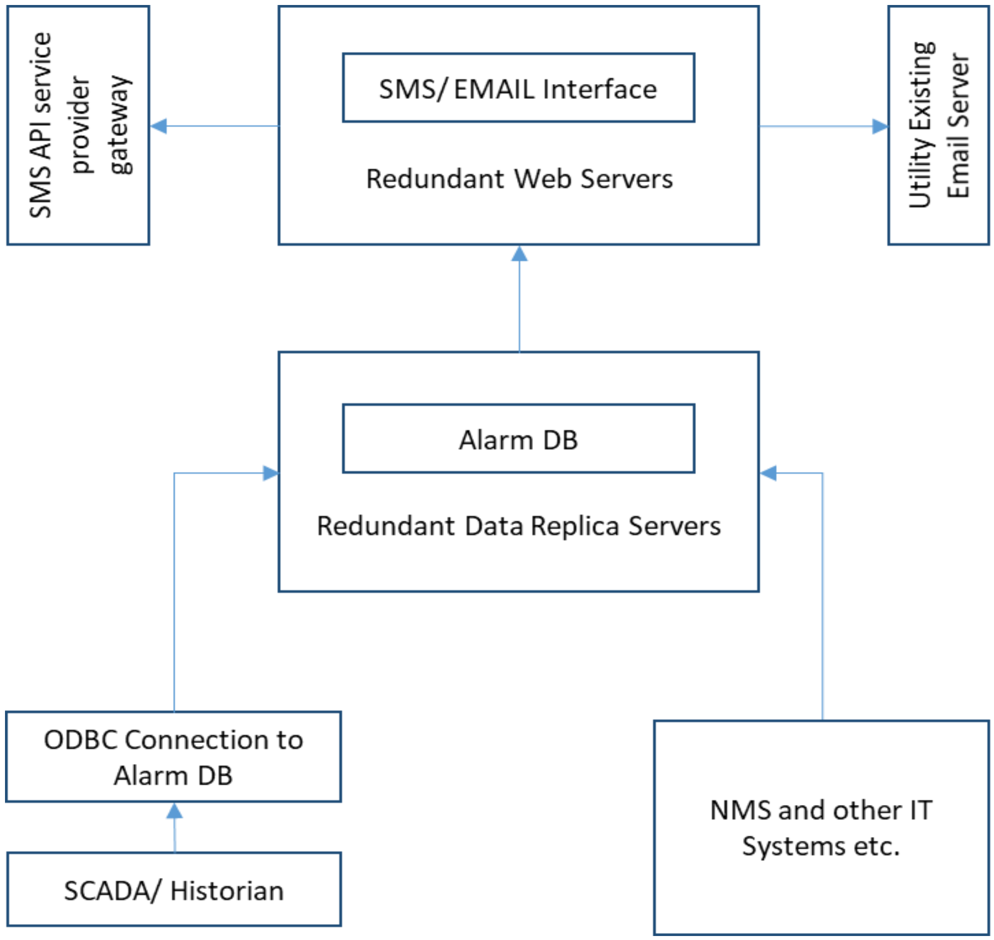


Figure 1 : Tentative architecture for SMS/Email interface functionalities

8.3 Web Services interface

Supplied system shall support Web Services that allows external user and application to interact with web applications and publish and subscribe any data. Web Services shall be accessible via standard Internet communication protocols like HTTP, XML and API based Interface also. Bidder shall supply .Net or Java based tool kit to create and configure services to publish data items name, values, Quality code, tag, time series of values etc.

----- End of Chapter8-----

Section 9
Cyber Security Requirements

Table of Contents

Section 9 Cyber Security Requirements

9.0 General requirements

This section describes the cyber security requirements of the entire SCADA/EMS system being procured which includes components such as firewall, routers, SIEM etc. This section also describes the functional and operational requirements of the cyber security systems/sub-systems being supplied. The system shall be compliant to "Cyber security in power sector guidelines 2021" issued by CEA and its latest amendment. The contractor has to ensure compliance with all the cyber security related statutory guidelines issued from time to time during the entire period of contract from all the regulatory bodies.

The SCADA/EMS system security features shall be designed to comply with the NCIIPC guideline for Critical Infrastructure Protection, ISO 27001, ISO 27019 and IS16335 standards as well as additional requirements specified herein.

9.1 Cyber Security System

A Cyber Security system shall be supplied by the Contractor for the cyber security requirements of the SCADA/EMS system. The contractor shall document and implement a Cyber Security Policy in line with Statutory latest guidelines to secure the system and the contractor shall keep updating the security settings as per the requirements by CERT-In/NCIIPC/CEA or any other Statutory Agency from time to time.

The following guidelines/strategies shall be taken care of for making the entire Control Centre resilient to all types of Cyber Threats and immune to Cyber Attacks.

(a) All the Hardware, Operating Systems (OS) and application software shall be hardened. **List of ports and services enabled in each hardware device must be shared after SAVT. This list must be updated periodically if any new ports/services are allowed or blocked after prior approval of Owner.**

(b) Network Zoning shall be implemented as per the proposed architecture given in Appendix-D of Part-A. However, the Contractor may suggest other methods of network architecture for enhanced security of the System.

(c) No user shall be allowed direct access from one network zone to another.

(d) All default user id & passwords shall be changed. All default user id & passwords shall be changed periodically in coordination with employer as per their policy. A well-defined password policy consisting of rules for forming password, sharing of passwords and password expiry etc. shall be finalized during detailed engineering. Default user settings shall enforce password complexity and usage rules.

(e) Logs of all network activities such as log in/log out; cable plug in/plug out etc. shall be created in the system.

(f) Latest Cyber Security Guidelines of statutory security agencies like CERT-In, NCIIPC, NIST, NTRO, CEA etc. shall be followed.

(g) The contractor shall identify and list out the entire network devices, servers and protocols that communicate with physical systems and limit what is not required.

(h) The contractor has to carry out bi-annual Cyber Security Audit by Cert-IN certified Auditors till the completion of the contract.

(i) Whitelisting policy shall be deployed for all port configuration, network routing, data flow, access etc. and all these details shall be documented **and any changes shall be recorded and informed to owner during entire period of contract.**

(j) The contractor shall document the baseline configuration and shall be reviewed annually and will be audited by the auditor.

(k) Antivirus protection for clients shall be provided.

(l) secure digital certificates shall be supported and configured to allow for single sign-on between Operating System and application system. This infrastructure shall allow customers to implement two-factor authentication into respective application system.

(m) Centralized log collection shall be implemented using SIEM, **which consolidates the logs from all the devices.**

(n) Remote Desktop Protocol and Network File Share on SMB protocol between devices shall be disabled

(o) Remote Access if required shall be done using Network Layer Authentication (NLA)

(p) Password Managers must be used to store passwords in encrypted format and use it to perform any logins into the system

(q) Any user created for system, or application shall not contain the word "admin" in it.

(r) Use endpoint security software to identify TTP events according to MITRE ATT&CK framework.

(s) Uniform IP address document shall be maintained.

(t) **For assessment of policies implementation in firewall/routers/switches necessary audit shall be conducted after site acceptance test (SAT) only.**

(u) **Policy implementation audit must be conducted periodically (quarterly) by the contractor and report to be submitted to owner.**

(v) **All the external traffic (RTU, ICCP, IT, OT etc.) destined to control centre shall be routed through firewall only.**

(w) **Automatic report/log generation for every device shall be provided.**

(x) **All the proposed cyber security products OEMs shall have their own threat intelligence platform.**

9.1.1 Cyber Security Policy

The Contractor shall document, finalize and implement a Cyber Security Policy in association/consultation with the Employer/Owner to secure the system in line with Government guidelines from CEA, CERT-In, NIST, NTRO, NCIIPC, any regulatory authority etc. The overall policy and implementation shall include but not limited to the following:

- Network partition and segmentation using Firewalls as required to achieve the desired level of the security of different Application system while facilitating smooth access for data and information to all type of users.
- Implement trusted, un-trusted and DMZ with clear perimeters.
- Prevent authorized users from reading or writing data or files, executing programs or performing operations without appropriate privileges.
- Document all user sign on procedure and auditing
- Auditing by CERT-In certified third-party during FAT, SAT and bi-annually during AMC period. **Each auditor along with the auditing firm need to be mandatorily changed after 3 consecutive audits so that different auditors audit the system throughout the maintenance phase including extension if any.** Contractor shall implement the recommendation/remedial actions suggested by the auditor after audit for any upgrade (Patches) in existing system.

  Note: For RLDC/SLDCs, Officers from CSIRT-Power will also be participating in the Cyber Security Audits (during FAT, SAT and bi-annually during AMC period)
- Maintain syslog for all servers & networking equipment logs and its integration with SIEM
- Mechanism to detect unauthorized/unusual activity and attempts to compromise system security based on logs of SIEM, NMS and Application logs. **The contractor to propose and document what constitutes normal activity/traffic periodically.**
- Unused ports (physical and logical) pf all devices such as on switches, routers, firewalls, consoles, servers, **HIPS etc**. shall be disabled.
- All the devices that connected to the system through LAN shall have mac-based

binding.

- Record all network traffic for detecting unauthorized activity, unusual activity and attempts to defeat system security (Contractor to propose and document what constitutes normal activity/traffic periodically (preferably yearly)).
- Auditing shall be carried out at minimum as per base line cyber security audit requirements specified by National Security council Secretariat.
- 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. All unused ports (physical and logical) of all devices e.g., routers, switches, firewalls, servers, workstations etc. shall be disabled.
- Third party software shall only be installed where required in consultation with employer/owner and after approval of competent authority.
- All unused default operating system users shall be disabled.
- Host-based firewalls shall be configured to only allow connections from specified nodes. Also, centralized management for these firewalls shall be provided.
- Applications white-listing approach shall be deployed in hosts to allow only whitelisted applications.
- All unused services shall be disabled by default. There shall be a provision to turn on all services on request.
- In routers & switches, only the specified/required IP addresses should be OPEN.
- **All the communication should be done through secure protocols such as SFTP, HTTPS etc.**
- Protection requirement shall also include but not limited to the following:
    - APTs and targeted attacks
    - Zero-day malware and document exploits
    - Web threats (exploits, drive-by-downloads)
    - Bots, Trojans, Worms
    - Key Loggers and Crime ware
    - Disruptive applications
    - Data exfiltration
    - Denial of service attacks
    - Protection against various threat to virtual and physical servers
    - Protection against ransomware
    - Any other attacks/virus/Trojans/threats/malware/vulnerabilities etc.

9.1.2 Remote Diagnostic

The remote diagnostic features shall be used in case of emergency only and with prior approval of owner/employer. Remote Diagnostic facility with necessary Hardware as required shall be provided for communication between the SCADA/EMS system at control center and the Contractor's & Employer/Owner's support office for the diagnosis of Hardware & Software problems. The remote logins shall be on secured network (such as SSL over VPN etc).

The login shall be protected by a user name & password entry. Two factor Authentication (OTP Based) should be done by using perimeter firewall. A SOP for remote diagnostic practice shall be designed and developed and accordingly SOP shall be followed for usage of remote diagnostic facility. The remote diagnostic facility shall also be equipped with capability to capture and store all generated logs pertaining user access, systems, applications, services, etc.

ISP will be provided and maintained by the owner however number of public IPs and bandwidth requirement to be indicated by the contractor.

9.1.3 Network Equipment

The features and configuration of the network equipment in the proposed system is mentioned in this section. The device configuration of all the network equipment shall be as per the latest Cyber Security guidelines given by CERT-In or any other statutory Organization.

9.1.3.1 Firewall

As per the proposed network architecture given in Appendix-D of Part-A, all the external, internal firewalls should be properly configured to segregate networks into different segments. Firewall shall have the features of Next Generation Firewall to secure the system more effectively. OEM of the firewall shall have their own Threat Intelligence Analysis Centre and shall use global footprint of security deployment for more comprehensive network protection. The firewalls should have the following features including requirements mentioned in respective DRS i.e. Appendix H.

- Application awareness and control: Firewall shall have the feature of identifying applications in the network and enforcing security policy at the application level itself.
- Identity awareness: Firewall shall have the feature of integrating with applications like active directory and enable firewall rules to individual users or user groups.
- Firewall shall be able to receive threat intelligence feeds from time to time to detect threats and prevent attacks.

Firewall shall provide easy integration with other devices like SIEM etc.

- Firewall solution shall support minimum 10000 IPS, minimum 2000 applications signatures and risk-based control that can invoke tailored IPS threat detection policy through optimized security effectiveness. These performance numbers must be available on Firewall Dashboard/GUI.
- Firewall device shall have the Geo-location based IPv4 & IPv6 database. So that Geo-location-based traffic filtering shall be done in the device. The device shall regularly update their Geo-Location base IPv4 & IPv6 database from the Global repository.
- Next Generation Fire Wall shall support on-premises sandboxing (Anti-APT, to be procured separately) feature to protect against zero-day attack if required in future.
- CVE (Common Vulnerabilities and Exposures) of Firewall OS shall be available /disclosed publicly in website.
- Firewall solution shall be purpose-built appliance and should not have wireless access and Bluetooth component within its hardware and software to facilitate direct connectivity (wirelessly) with firewall.

  Firewall solution shall provide IPv4 and IPv6 dual stack support from day one and Firewall OEM should be IPv6 Ready logo approved.
- The proposed Firewall / Firewall Operating System shall be tested and certified for **EAL4**+/ NDPP (Network Device Protection Profile)/NDcPP (Network Device Collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, DEIT, Govt. of India.

The following strategies shall be followed for secure configuration of firewalls.

- Clean-up rule.
- Place a 'Deny Any-Any' rule at the end of the rule base.
- Never create an 'Allow any-any' rule.
- Allow rules should be created only for required services.

This will result in all traffic being disallowed, unless specifically allowed.

- Lockdown/stealth rule
- All traffic destined for the firewall itself should be disallowed.
- Anti-spoofing rule.
- Place anti-spoofing rule as per RFC 1918 and 2827.
- Enable DoS/DDoS features on Firewall

- Enable application-level filtering of firewall
- It should show policy traffic trend over the day with host and destination addresses by selecting on each policy
- **Geofencing shall be enabled in all the firewalls and security devices.**

9.1.3.2 Router

Necessary control shall be applied on the router to stop unwanted traffic and attacks at the perimeter itself. In the secure configuration of a router, the strategies not limited to following shall be considered.

- Deploy proper access management and avoid remote administration.
- Enable secret password.
- Change default SNMP community string.
- Turn on logging to a central SIEM
- ACLs (Access Control Lists) should include
    - Apply egress/ingress filter
    - Filter all RFC 1918, 3330 address space and special/reserved address
    - Permit the required services for the required IP addresses only
    - Deny everything else.
    - Area segregation must be implemented (if OSPF is being used) between internal and external networks. Appropriate protocols must be enabled to prevent networks loops.

9.1.4 Intrusion Detection & Prevention System

The required features of the Host Based Intrusion Detection and Prevention System (HIPS) and Network Based Intrusion Detection Prevention System (NIPS) are described below:

a) Intrusion Detection and Prevention System (Host Based)

Host based Intrusion Detection and Prevention System module shall be provided for all machines on DMZ LANs and machines interacting from outside the network. IDS shall be able to perform following actions:

- Capability for Detecting the intrusion attempt that may take place, intrusion in progress and the intrusion that has taken place.
- Flag and check unauthorized access

- Notify/Alarm/message of intrusion to:
- Management console
- Event log
- Administrator by e-mail

- Create an 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 by unauthorized account or there is an un-authorized attempt to overwrite vital system files, to install Trojan horses or backdoors, suitable action should be taken such as:

    - Terminate User (intruder) directly or through Active directory, SIEM etc.
    - Login Disable User (intruder) Account directly or through Active directory, SIEM etc.
    - Forge a TCP FIN packet to force intruder connection to terminate

- Shall provide events check for suspicious file transfers, denied login attempts, physical messages (like an Ethernet interface set to promiscuous mode) and system reboots etc.

b) Network based Intrusion Prevention System (NIPS)

The NIPS shall provide complete inline protection from network-based application layer threats by scanning packet payloads for malicious traffic. It shall detect,classify and stop malicious application, viruses, worms and spyware/adware etc. After detecting an intrusion attempt NIPS should be able to perform following actions:

- Suggest/Reconfigure changes in the firewalls provided in this package
- Send an SNMP Trap datagram to the management console.
- Send an event to the event log.
- Send e-mail to the administrator to notify the attack.
- Save the attack information (timestamp, intruder IP address, victim IP address/port, protocol information)
- Force intruder connection to terminate.
- NIPS shall have capability to detect various operating system of

devices/servers running on the network and profile them for more visibility and protection (for impact assessment & vulnerability analysis)

9.1.5 Security Information and Event management (SIEM)

A dedicated system called SIEM shall be deployed having following features:

- SIEM tool shall offer a single, unified view for all logs generated across the SCADA/EMS network.
- SIEM system shall be easy to install, configure, use and maintain.
- SIEM shall have pre-built dashboard containing statistical information about the complete system. There shall be a feature to create customized dashboards to organize and correlate multiple data sources visually in a single user interface.
- Complete network-based scanning enabling assessment and analysis of threats impacting network.
- Robust Log data warehouse that enables creation and sharing of reports on all aspects of the system's remediation efforts in support of policy compliance.
- Create custom remediation packages to address recurring configuration issues, remove unauthorized files and applications, and patch software.
- Configurable monitoring to enable Regulatory and standards-based assessment of end points compliance
- Continuous Monitoring - continuously collect detailed status information on all critical cyber assets and immediately detect any changes.
- Automated Assessment - automatically aggregate and analyze security data and raise alert on suspicious events or modifications that impact compliance status.
- Audit-ready Evidence - Quickly generate reports and update dashboards that provides transparent overview of the systems by requirement, compliance with security controls and processes.
- SIEM solution shall be able to integrate with all security solutions provided including Firewall, Server security and Endpoint security solutions through standard protocols.
- The solution shall be able to not only detect threat but also shall be able to recommend appropriate response.
- SIEM shall use a variety of advanced detection and investigative controls to detect abnormal activity which is often associated with any compromised systems.

9.1.6 Application Whitelisting tool

A tool (separate or part of NAC or End Point security solution) shall be provided by the contractor for ensuring that only required software are running on the system being procured. Contractor along with employer/owner shall specify whitelist of applications which are required for the proper functioning of SCADA/EMS system. The features of this tool are: This tool shall run in all nodes i.e., servers, workstations.

- Tool shall be able to discover applications running in the network and shall provide list of application running on all nodes i.e., servers and endpoints.
- Tool shall be able to select required applications from the list of installed applications on the node.
- This tool shall run in default deny mode i.e., all applications are blocked from execution by default and only the whitelisted applications shall be executed.
- Tool shall be able to whitelist application builds (groups) and updates the whitelist automatically based on the discovered applications' compliance with organization's selected policies like trusted vendors/ product name/folder path.
- This tool shall not impact the availability and performance of SCADA System in any scenario.
- An alert shall be generated on the corresponding node, when any application is blocked by the tool and the same shall be logged for future reference. The same shall be notified to user with email/SMS.
- User (System Admin) shall have the privilege to update/modify the whitelisting tool without any impact on the running system.
- All the changes in the whitelist shall be logged.
- Facility to download the current whitelist configuration of the tool shall be available in format such as CSV, PDF, XML etc.
- By default, the tool shall be enabled in all the nodes. User shall have the privilege to enable/disable the tool in any particular node depending upon the requirement. Clear log shall be maintained about the time period for which the tool is disabled along with details.

Generic architecture of Application Whitelisting tool is given in **Appendix -B.**

9.1.7 End Point Security Solution (Antivirus)

All computers and firewalls shall be provided with the latest End Point Security software as on date of supply. This software shall have the capability of having its virus definitions updated from time to time. This software shall have the feature to integrate with other devices like SIEM, firewall etc.

The Contractor shall be responsible for the maintenance & update of the software. Additionally, it shall have the facility to enable control on USB ports for disabling unauthorized usages. Its functional specifications shall be as follows: It shall block USB devices based on device identity, port identity, device type (e.g., allowing all keyboards, etc.) A provision for listing acceptable devices (white-listing) shall also be provided. It shall log all USB port access events. **(Capturing details of connected USB). It shall allow only identified USB devices to connect to a computer system. It shall have configurable firewall features.**

9.1.8 Software update and Patch Management tool

The Contractor shall be responsible for the maintenance & update of the patches, firmware and signatures of Operating system, entire SCADA/EMS system, Firewalls, Networking Equipment during the entire period of contract **including extension of contract, if any.**

Patches shall be downloaded from authentic sources in patch management server that is available in DMZ zone. After successful downloading it shall be transferred to patch management server in PDS Lan, where all the patches will be tested. After successful testing of the patches, it shall be distributed to the entire system.

Automated patch management tools shall be provided to facilitate the distributions of relevant patches to the entire system. Patches should be applied to all the devices & software delivered in the project. The contractor shall also be responsible for providing updates/patches for all the software products supplied under the project for the entire period of the contract **including extension of contract, if any.**

9.1.9 Database Development System (DDS)/Program Development System (PDS) as a test bench for Cyber Security Requirement

A Test bench PDS i.e. (as specified in section 4.3.6) PDS shall be delivered by the Contractor. Along with functions defined in that section, this will be used for following purposes also-

a) This system shall also be used as a Test bench for Cyber security and shall accordingly be equipped with firewall, antivirus and enable mode wherein threat scenarios can be tested with configured security elements before implementing on the main/production system.

b) This Test bench for Cyber security shall also be used for VAPT (Vulnerability Assessment & Penetration Tests) e.g., OS fingerprinting, Port scanning, etc.

9.1.10 Tool for VAPT

A tool shall be provided by the contractor for conducting VAPT on regular basis in SCADA/EMS Network. It shall have feature to be installed on server or workstation or laptop as per the Owner requirements. Features of this tool are:

- This tool shall be able to scan and detect vulnerabilities in all the assets in the network. The assets shall include but not be limited to the following:
    a) Network devices (firewalls, router, switches etc)

b) Operating Systems (Desktop OS and Server OS) (Support for Windows, Linux, MAC, Unix)

c) All software applications including Database

- This tool shall be able to create customized reports like reports based on e.g., specific vulnerability types, vulnerabilities by host/plugins – in a variety of formats like CSV, PDF, XML etc.
- This tool shall be easy to set-up, use and maintain.
- The contractor shall be responsible for vulnerability management. A define process shall be followed to fix/meet vulnerability identified in a deployed system, device, configuration, application, service, etc.
- Quarterly VAPT shall be performed by contractor with this tool and vulnerabilities to be fixed accordingly. The VAPT may be performed as and when required by Owner.
- Updates of the VAPT tool shall be provided regularly.

-----End of section 9-----

APPENDICES for TS

Vol. II, Part-B
Appendix - A
GLOSSARY

Appendix A

GLOSSARY

Name	Definition
AC	Alternating Current
ABT	Availability Based Tariff
ACM	Alternating Current Model
A/D	Analog-to-Digital
ADC	Analog-to-Digital Converter
AGC	Automatic Generation Control
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Exchange
APS	Auxiliary Power Supply
ATC	Available Transmission Capability
ATM	Analog Tele-measurement
AVR	Automatic Voltage Regulation
BCC	Backup Control Centre
BDF	Bus Load Distribution Factors
BLF	Bus Load Forecast
BOQ	Bill of Quantity
BSPTCL	Bihar State Power Transmission Company Limited
CA	Contingency Analysis
CADD	Computer Aided Drafting and Design
CB	Circuit Breaker
CCAPI	Control Centre Application Program Interface
CEA	Central Electricity Authority (India)
CERC	Central Electricity Regulatory Commission
CERT-In	Computer Emergency Response Team- India
CIM	Common Information model
CMIP	Common Management Information Protocol
COP	Current Operating Plan
CPCC	Central Project Control Centre

CPU	Central Processing Unit
CS	Central Sector
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DAC	Digital-to-Analog Converter
DAT	Digital Audio Tape
DC	Direct Current
DDS	Database Development System also used for Database Development System as a test bench
DM	Differential Mode
DMS	Document Management System
DOT	Department of Telecommunications
DSA	Dynamic Security Assessment
DVC	Damodar Valley Corporation
DTM	Digital Tele-measurement
DTS	Dispatcher Training Simulator
ED	Economic Dispatch Function
EHV	Extra High Voltage
EMS	Energy Management System
EPAX	Electronic Private Automatic Exchange
EPRI	Electric Power Research Institute
ERLDC	Eastern Region Load Dispatch Centre
F	Frequency
FAT	Factory Acceptance Test
FACTS	Flexible A.C. Transmission System
FO	Fiber Optic
FTP	File Transfer Protocol
FTS	File Transfer Spool
FSP	Forecasting Service Provider
GPS	Geographic Positioning System
GRID-INDIA	Grid Controller of India Limited (formerly known as Power System Operation Corporation Ltd.)
GUI	Graphics User Interface
HI	Historical Information Function

HS	Hydro Scheduling Function
HSM	Hydro System Model
HTC	Hydro-Thermal Coordination Function
HV	High Voltage
HVAC	High Voltage Alternating Current
HVDC	High Voltage Direct Current
I	Current
ICCCM	Inter-Client Communications Conventions Manual
ICCP	Inter-Control Center Communications Protocol
IEEE	Institute of Electrical and Electronics Engineers Inc.
IEC	International Electro Technical Commission
IF	Inflow Forecasting Function
IHR	Incremental Heat Rate
I/O	Input/output
IPv4	Internet Protocol version-4
IPv6	Internet Protocol version-6
IPP	Independent Power Producer
IS	Interchange Scheduling Function
ISGS	Inter-State-Generating-Station
ISO	International Standards Organization
ISR	Information Storage and Retrieval Function
IST	Indian Standard Time
ISTS	Inter State Transmission System
ITE	Interchange Transmission Evaluation Function
JUSNL	Jharkhand Urja Sancharan Nigam Limited
LAN	Local Area Network
LDC	Load Dispatch Centre
LD&C	Load Dispatch and Communication
LAN	Local Area Network
LDCs	Load Dispatch Centers
LDAP	Lightweight Directory Access Protocol

LED	Light-Emitting Diode
LF	Load Forecasting
LSS	Load Shed Support
MCC	Main Control Centre
MC	Monitoring Centre
MMI	Man Machine Interface
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NACK	Negative Acknowledgement
NC	Normally Closed- Circuit Contact
NCIIPC	National Critical Information Infrastructure Protection Centre
NERC	North American Electric Reliability Council
NHPC	National Hydro-Electric Power Corporation Limited
NLDC	National Load Dispatch Centre
NPC	Nuclear Power Corporation
NRLDC	Northern Region Load Dispatch Centre
NSP	Network Status Processor
NTP	Network Transfer Protocol
NTPC	National Thermal Power Corporation Limited
OHL	Overhead Line
OLTC	On Load Tap Changer
OM	Operations Monitor
O&M	Operation and Maintenance
OPF	Optimal Power Flow
OPTCL	Odissa Power Transmission Corporation Lomited
OS	Outage Scheduler Function
OSI	Open Systems Interconnection
P	Active Power
PABX	Private Automatic Branch Exchange
PAF	Plant Availability Factor
PAS	Power Application Software

PC	Personal Computer
PCB	Printed Circuit Board
PDC	Phasor Data Concentrator
PLCC	Power Line Carrier Communication
PMU	Phasor Measurement Unit also referred as synchro phasor
POWERGRID	Power Grid Corporation of India Limited
PS	Production Statistics Function
PSA	Power System Analysis Function
PSM	Power System Model
PSMU	Power System Model Update function
PVC	Polyvinyl Chloride
Q	Reactive Power
RC	Remote Console
RDBMS	Relational Data Base Management System
RDCC	Reports Data Collection and Calculation function
RM	Reserve Monitoring
REB	Regional Electricity Board
RLDC	Regional Load Despatch Centre
RRVPNL	Rajasthan Rajya Vidyut Prasaran Nigam Limited
RPC	Reactive Power Controller
REMC	Renewable Energy Management Centre
RLDC	Regional Load Despatch Centre
RMA	Return Merchandise Authorization
RTU	Remote Terminal Unit
SAS	Substation Automation System
SAT	Site Acceptance Test
SCA	Short Circuit Analysis
SCADA	Supervisory Control and Data Acquisition
SCS	Small SCADA System
SE	State Estimator
SEB	State Electricity Board

SERC	State Electricity Regulatory Commission
SIC	Signal Interface Cabinet
SMTP	Simple Mail Transfer Protocol
SOE	Sequence-of-Events
SLD	Single Line Diagram
SLDC	State Load Dispatch Center
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
STPS	Super Thermal Power Station
SVC	Static VAR Compensator
TAC	Technical Assistance Contract
TB	Terminal Block
TCM	Transmission Line/Corridor Capability Monitor
TCP/IP	Transmission Control Protocol / Internet Protocol
TCPAR	Thyristor Controlled Phase Angle Regulator
TCSC	Thyristor Controlled Switched Capacitor
TEC	Tata Electric Company
TLF	Transmission Loss Sensitivity Factors function
TM	Tele measurement
TPS	Thermal Power Station
TTC	Total Transmission Capability
UC	Unit Communication Function
UCA	Utility Communication Architecture
UI	User Interface
UPS	Uninterruptible Power Supply
URTDSM	Unified Real Time Dynamic State Measurement
UTC	Used Transmission Capability
VDU	Video Display Unit
V	Voltage
VPS	Video Projection System
VT	Voltage Transformer

WAN	Wide Area Network
WSP	Weather Service Provider
WBSETCL	West Bengal State Electricity Transmission limited

VOL. II, PART-B

APPENDIX - B

SAMPLE REPORTS & DISPLAY FORMATS

APPENDIX - B

SAMPLE REPORTS AND DISPLAY FORMATS

This SCADA/EMS appendix contains the format requirements for a number of typical Reports/Displays as part of SCADA/EMS system. Report/display shall not have any sizing limitations (software) except the hardware processing resources if any.

Reports/Displays generation software shall provide the capability to add future points as it becomes necessary. Delivered system shall include total storage for 10 times the space required for the reports/displays defined in this appendix.

NOTE: Reports and Display format is for sample purpose and it may vary on site-to-site basis as per local requirement.

B1. (A)Data Availability Reports

i. Control Centre wise Analog /Digital Data Availability report

A	B	C	D	E	F	G	H	I	J
Summary of Telemetry Availability (Analogs) at 765 kV Sub - Stations									
Sl. No.	**Region**	**Regional Transmission system**	**Name of sub-stations**	**Total no. of Analogs**	**Total no. of Analogs Integrate**	**Total no. of Analogs not-integrated**	**Non-Availability in a Station**	**Non-Availability in respective**	**Non-availability in a Region**
1	**NR**	**NRTS-2**	Moga	20	18	2	10%	**8%**	**7%**
2			Bhiwani	24	11	1	4%		
3			Jhatikara	21	19	2	10%		
4		**NRTS-1**	Fatehpur	23	23	0	0%	**5%**	
5			Agra	26	22	4	15%		
6			Balia	18	17	1	6%		
7			Meerut	18	18	0	0%		
8			Bareilly	11	11	0	0%		
9			Varanasi	21	20	2	10%		
10			Kanpur	21	21	0	0%		
11			Lucknow	16	16	0	0%		
12		**UPPCL**	Anpara-C	20	17	3	15%	**9%**	
13			Unnao	17	16	1	6%		
14			Greater Noida	20	19	1	5%		
15			Anpara-D	17	15	2	12%		
16		**RRVPNL**	Anta	18	16	2	11%	**13%**	
17			Phagi	29	25	4	14%		

ii. Station wise Analog /Digital Data Availability report

DETAILED DATA AVAILABILITY STATUS OF 765 KV STATION — Annexure - II

Sl. No.	STATION NAME	ELEMENTS NAME	ANALOG					STATUS			REMARKS		
			MW	MVAR	VOL	FREQ	OLTC	CB (Total)	CB (Avl)	ISO	Integration Status	Reason for non-availability.	Comm. / Data Status.
1	MOGA	765kV Bus 1	-	-	YES	YES	-						
		765kV Bus 2	-	-	YES	YES	-						
		765kV Moga-Bhiwani Line	NO	NO	-	-	-	1	0				
		Tie bay Bhiwani Lin& ICT6						1	0				
		ICT6	YES	YES			YES	1	0				
		765KV Moga-Kishenpur1 Line	YES	YES				1	0				
		Tie bay Kishenpur1 & Bus Reactor						1	0				
		Bus Reactor 1, 3x80 MVAR	-	YES				1	0				
		765KV Moga-Kishenpur2 Line	YES	YES				1	0				
		Tie bay Kishenpur2 & Bus Reactor						1	0				
		Bus Reactor 2, 3x80 MVAR	-	YES				1	0				
		765KV Moga Meerut-1 Line	YES	YES				1	0				
		Tie bay Meerut-1 Li& ICT5						1	0				
		ICT5	YES	YES			YES	1	0				
		Sub-Total	6	8	2	2	2	12	0				
		Total Measurents	20					12					
		Total Available Measurents	18					12					
		Total Non-Available Measurents	2					0					
		Total Suspect Measurents	0										
		Total Measurents Not Configured	0										
		% of Suspect	0%										
		% of Not Configured	0%										
		% of Non-Availability	**10%**					0%					

RTU WISE ANALOG & DIGITAL POINTS AVAILABILITY REPORT

	ANALOG POINTS		DIGITAL POINTS(CB)		DIGITAL POINTS(ISOLATOR)		DIGITAL POINTS(PRT)	
RTU/Gatewayname	TOTAL MAPPED IN DATABASE	TOTAL AVAILABLE IN GOOD	TOTAL MAPPED IN DATABASE	TOTAL AVAILABLE IN GOOD	TOTAL MAPPED IN DATABASE	TOTAL AVAILABLE IN GOOD	TOTAL MAPPED IN DATABASE	TOTAL AVAILABLE IN GOOD
RTU1								
RTU2								
….								
RTUn								

B1. (B) RTU & Channel Availability Reports

i. RTU Availability Report

RTU_NAME	RTU_AVAILABILITY
ARSUR	99.81
BDADI	100.00
BHDVT	99.73
CDDPA	100.00
COSTL	100.00
GHNPR	99.97
GJWKA	100.00
GOOTY	100.00
HASAN	100.00
HIRYR	100.00
HOSUR	100.00
ILFS4	89.88
KAIGA	99.95
KARKD	99.78
KDKLM	100.00
KHMAM	100.00
KLPKM	99.65
KLVPT	100.00
KMKLM	100.00
KOCHI	100.00
KRNL7	99.79
KZKDE	99.95
LANCO	100.00
MDGRI	99.64
MDURI	100.00
MEPL	99.93
MNRBD	99.99
MYSOR	100.00
NCC	100.00
NGPTM	100.00
NLRPS	100.00
NLTS2	99.94
NLY1E	100.00
NLY2E	100.00
NRNDR	100.00
NSGAR	99.79
NTPL	100.00
NUNNA	100.00
PLKAD	100.00

ii. Channel Availability Report

RTU/Gateway name	Primary channel		Secondary channel	
	% availability	% of time RTU was on this channel	% availability	% of time RTU was on this channel
RTU 1				
RTU 2				
RTU 3				
RTU 4				
….				
RTU n				

- Provision of displaying two separate communication routes/channels in existing SCADA system front end display should be made indicating if one of the route/channel gets turned off

B1. (C) ICCP link Availability Report

MAIN SRLDC ICCP LINK STATUS			
Date	21/04/2020		
SL No.	ICCP SITE	LINK PROTOCOL UP (YES/NO)	
		LINK-1	LINK-2
1	NLDC MAIN	YES	YES
2	NLDC BACKUP	YES	YES
3	SRLDC BACKUP	YES	YES
4	KPTCL	YES	NA
		P2P	RING
5	TANTRANSCO MAIN	YES	NO
6	APTRANSCO MAIN	YES	YES
7	TSTRANSCO MAIN	YES	YES
8	KSEB MAIN	YES	YES
9	PUDU MAIN	YES	YES

B1. (D) SoE Report

The below mentioned report is the prototype only. Sorting filtering feature is required as per the specifications mentioned in the section: 1 under 1.4 "Sequence of Events"

HIST_TI	ABNOR	AREA	CATEG(	LOCATION	TEXT	TIME
18:50:10	1	KASEB	1P	NGJHR_KA	NAGJHARI UNIT UNIT G3 AUTO	18:50:06
18:19:20	1	KSEB	1P	LPYR2_KL	LOWER PERIYAR UNIT UNIT G3 AUTO	18:19:16
18:03:00	0	KSEB	1P	KKYM1_KL	KAKKAYAM UNIT UNIT G6 MANUAL	18:02:50
18:01:00	1	KSEB	1P	KKYM1_KL	KAKKAYAM UNIT UNIT G6 AUTO	18:00:56
17:56:40	1	TSTRAN	1P	JGPD4_AT	JULURUPADU 400 CB TIE 14 - CB 41452 NORMAL	17:56:37
17:56:40	1	TSTRAN	1P	JGPD4_AT	JULURUPADU 400 CB TIE 17 - CB 41752 NORMAL	17:56:37
17:56:40	1	TSTRAN	1P	JGPD4_AT	JULURUPADU 400 LINE 400Kv LINE 1 to SRPT4 NORMAL	17:56:37
17:56:40	1	TSTRAN	1P	JGPD4_AT	JULURUPADU 400 LINE 400Kv LINE 2 to SRPT4 NORMAL	17:56:37
17:34:00	1	TANTCO	1P	NLTS2_CS	NEYVELI TS-II UNIT UNIT G4 AUTO	17:33:52
17:32:30	1	TANTCO	1P	PGRDC_PG	PUGALUR HVDC CB TIE 22 - CB 42252 NORMAL	17:32:25
17:32:30	1	TANTCO	1P	PGRDC_PG	PUGALUR HVDC CB REACTOR CB 43152R NORMAL	17:32:25
17:32:30	1	TANTCO	1P	PGRDC_PG	PUGALUR HVDC CB TIE 32 - CB 43252 NORMAL	17:32:25
17:32:30	1	TANTCO	1P	PGRDC_PG	PUGALUR HVDC CB REACTOR CB 43252R NORMAL	17:32:25
17:32:30	0	TANTCO	1P	PGRDC_PG	PUGALUR HVDC CB TIE 22 - CB 42252 TRIP	17:32:21
17:32:30	0	TANTCO	1P	PGRDC_PG	PUGALUR HVDC CB REACTOR CB 43152R TRIP	17:32:21
17:32:30	0	TANTCO	1P	PGRDC_PG	PUGALUR HVDC CB TIE 32 - CB 43252 TRIP	17:32:21
17:32:30	0	TANTCO	1P	PGRDC_PG	PUGALUR HVDC CB REACTOR CB 43252R TRIP	17:32:21
17:00:30	0	TSTRAN	1P	CDLP4_AT	CHANDULAPUR 400 XFMR_P 40_T1 (Primary) TRIP	17:00:29

Time	Name of State	Name of Substation	Name of equipment