NEPAL ELECTRICITY AUTHORITY

(An Undertaking of Government of Nepal)
Project Management Directorate
Distribution Line and Substation Department

NEA DIGITAL NETWORK AND SCADA EXPANSION PROJECT

BIDDING DOCUMENT
FOR

Procurement of Plant for
Design, Supply, Installation and Commissioning
of
NEA Digital Network and SCADA Expansion
(Procurement of Plant)

Single-Stage, Two-Envelope
Bidding Procedure

Issued on:	**22nd February 2026**
Invitation for Bids No.:	**PMD/ETDSSP/NDNSEP-082/83-01**
OCB No.:	**PMD/ETDSSP/NDNSEP-082/83-01**
Employer:	**Nepal Electricity Authority**
Country:	**Nepal**

VOLUME –II (Part-A)

NEA Digital Network & SCADA Expansion Project
Distribution Line and Substation Department
Project Management Directorate
Matatirtha, Kathmandu, Nepal
Telephone: 01 5164099

(Volume -II, Part-A)
PSR & Technical Specifications

Table of Contents

CHAPTER 1: PROJECT SPECIFIC REQUIREMENTS

.

1. Background

The Nepal Electricity Authority (NEA) is a comprehensive power generation, transmission, and distribution organization that provides electricity services throughout Nepal. Established on August 16, 1985, under the Nepal Electricity Authority Act of 1984, NEA was formed through the merger of the Department of Electricity, the Ministry of Water Resources, the Nepal Electricity Corporation, and various development boards.

NEA's primary objective is to generate, transmit, and distribute adequate, reliable, and affordable power. This involves planning, constructing, operating, and maintaining all generation, transmission, and distribution facilities within Nepal's interconnected and isolated power systems. In addition to this core mission, NEA has several key responsibilities:

- To advise the Government of Nepal on long- and short-term plans and policies related to the power sector.
- To recommend, determine, and implement the tariff structure for electricity consumption, subject to prior approval by the Government of Nepal.
- To facilitate capacity building to develop skilled manpower in generation, transmission, distribution, and other related sectors.

As part of its ongoing modernization and digitalization initiatives, NEA is implementing several key infrastructure strengthening projects, Smart Metering in the Kathmandu Valley, Undergrounding in Kathmandu valley, Pokhara, and Bharatpur districts, the establishment of a Distribution Command and Control Centre at Syuchatar, and Disaster Recovery Centre (DRC) at Butwal. NEA is also deploying SCADA/DMS/OMS systems across 30 Distribution Substations in the Kathmandu Valley and implementing Substation Automation Systems (SAS) across six Grid Division Offices nationwide.

To enable these advanced Infrastructure, NEA has strengthened its communication backbone through continuous deployment of Optical Ground Wire (OPGW) along major transmission corridors and installation of SDH transport equipment in Grid Substations. These efforts have created a robust communication network essential for system reliability, automation, and future digital expansion.

NEA plans to implement SCADA in its Distribution Substations and connect its substations through enhanced fiber-optic connectivity using future ready telecommunication technologies. This seamless, high-speed communication network will support NEA’s existing and upcoming applications, ensuring real-time data availability, improved system reliability, and granular operational visibility across Distribution and Grid substations, critical for cross-border power trading, Local control and data-driven decision-making.

The project is being implemented with financial assistance from the Asian Development Bank (ADB) under the SASEC Electricity Transmission and Distribution Strengthening Project (SASEC-ETDSP).

The specification outlines the technical requirements for SCADA, telecommunication systems, and associated equipment to be supplied, installed, tested, and commissioned on a turnkey basis,

enabling NEA to establish a reliable, future-ready digital power network for Nepal.

2. Scope of Work

The overall Scope of Work assigns the successful System Integrator (SI) **single-point responsibility** for the entire integrated system, covering the survey, design, engineering, procurement, supply, installation, testing, commissioning, operation, and maintenance of an integrated SCADA and Telecommunication system across all existing and under-construction substations of Nepal Electricity Authority (NEA).

(a) **Project Components:** The scope explicitly includes the distribution SCADA solution (Software and hardware), LDMS, Fiber, IT & OT Networks (DWDM & OTN), and NOC Infrastructure.

(b) **Total Support Term:** The Contractor's overall support responsibility (including defect liability and FMS) shall extend over seven (7) years from the commencement of the project (DLP, 5-year Warranty, and 4-year FMS/AMC/ATS).

(c) **Deemed Inclusion:** Any element not explicitly mentioned but necessary for successful commissioning and functioning to meet NEA's operational requirements shall be deemed included in the SI's scope without any additional cost.

The project components are broadly categorized as follows:

- **Part A:** This covers the deployment of the core network systems, optimized for resilience and security. The SI shall design **two physically and logically separate, redundant fiber rings**:
  - The **OT Network (OTN)**: Forming the primary communication medium for time-critical SCADA data.
    - **Optical Transport Network (OTN):** As the primary communication medium for SCADA data, and NEA internal applications forming a resilient IT Ring.
  - The **IT Ring (DWDM):** Forming the high-capacity transport backbone for NEA internal applications.
    - **DWDM:** NEA private network, forming a separate OT Network.
  - **GPRS Technology:** communication medium for SCADA secondary communication ensuring SCADA connectivity is available until and beyond fibre availability.
  - **Network Operation Centers (NOCs):** Deployment of dedicated NMS and eestablishment of dedicated NOCs for monitoring of the SCADA, IT and OT networks including ADSS, respectively with a centralized IT infrastructure and a 24/7 operational setup.
- **Part B:** This covers the application layer, central intelligence, and field device integration, adhering to the required capacity limits.
- **SCADA Software and Applications**
  - **Licensing & Expansion:** All software licenses shall be perpetual, registered in NEA's name, and free of limitations on the number of substations, data points, or signals, capable of future expansion without additional license cost.
  - **System Sizing:** The Distribution SCADA system (DCC/DRC) must be sized to manage 215 total Distribution Substations (DSs) estimating the below I/Os, however, the total count of I/Os shall be finalized by the successful bidder post field survey. **The System shall be licensed for an initial capacity of at least 150,000 data points, expandable**

to 250,000 points without software architecture changes.

- The ultimate sizing expected during the 7-year project duration which would be frozen post final survey/analysis of the distribution system and interactions with DCSD at T+30 months. This quantity will be considered for OPERATIONAL ACCEPTANCE.
- **Application Scope:** The SI shall supply and install SCADA/FEP, Historian, DTS, ISR, and LDMS applications.

- **Field and Legacy Integration Mandates**
  - **ICCP Integration**: The software shall enable integration with external control centers on ICCP (TASE.2 or higher), specifically supporting 10 ICCP links to integrate the 6 regional Grid MCCs (Published Scope available on NEA Procurement Portal), LDC, DCC, and DRC/BCC.
  - **Protocol Compliance:** The system must be compliant with IEC 60870-5-104/101, IEC 61850, DNP 3.0, and DLMS/IEC 62056 for seamless interoperability.
  - **Existing Asset Integration:** The scope includes integrating data from existing SCADA, DMS, and OMS applications catering to 30 SS in Kathmandu Valley (Published Scope available on NEA Procurement Portal), existing 18 SS where Distribution SAS (Published Scope available on NEA Procurement Portal), is implemented, upcoming GIS application, upcoming country Wide DMS/OMS application, and approximately 50 RTUs, FRTUs procured under various projects.
- **Real-time Monitoring and Control – Distribution SCADA.**
  - Implementation across all distribution substations, including Remote Terminal Units (RTUs) and central systems at the Data Center (DC) and Disaster Recovery Center (DRC). SCADA NMS will be used to monitor all the nodes of the SCADA system.
- **Part C:** Fiber Connectivity Expansion – ADSS connectivity to substations and distribution consumer service centres (DCS) as a primary medium for IT&OT Networks.

2.1 Broad Scope of Work

The SI, in coordination with NEA, shall be responsible for the end-to-end execution of the project, including:

- Site survey, design, and detailed engineering
- Procurement, supply, and delivery of all materials and equipment
- Installation, integration, and commissioning of the complete system
- System acceptance testing and Go-Live support
- Operation, maintenance, and capacity building for NEA

The scope broadly covers the following key areas:

a) Survey, Design & Planning:

Site and Route Survey:

- Conduct detailed route surveys of all distribution and transmission substations, optical fiber paths, and propose Single line diagrams for ADSS stringing on HT/LT distribution lines and SCADA substation locations for approval.
- Survey all sites (Substations, DCS, DC, DRC, DCC, BCC) to determine exact placement,

space, and power needs for SCADA RTUs, OTN/DWDM equipment, and identification of PoPs (Point of Presence for DWDM locations).

- Identify specific substation locations lacking fiber path access that will require GPRS modems for RTU communication.

System Architecture Design:

- Develop a comprehensive system architecture for the integrated SCADA and communication networks. The SCADA architecture should be modular and logically separable to incorporate the SS under the 7 provinces in NEA without the need to add additional DB licenses.
- Design two physically and logically separate, redundant fiber networks: the OT Networks (OTN) for SCADA data and the IT Network (DWDM) for other IT services.
- Design Core, Aggregation, and Pre-Aggregation PoPs (Point of Presence) ensuring equipment redundancy at Core PoPs and power redundancy at all PoPs.
- Optimize the network design for service availability and assured Quality of Service (QoS).
- The new OTN/DWDM deployment must interface with and potentially augment/replace the existing SDH equipment utilizing the existing fiber core based on the survey report duly approved by NEA.
- The overall network is designed considering the critical network design parameters i.e. Scalability, Security, Manageability, Reliability, Interoperability and Resiliency requirements.
- The core network shall be created with required redundancy. Hence a ring architecture shall be the choice for the network topology. All rings shall be created by using transmission routes to the extent possible. In case ring closure is not feasible through transmission circuits, it shall be done through distribution poles.
- SI shall ensure that network design and implementation must be free of any SPOF (Single Point of Failure) from perspective of both active and passive elements. Considering the scope set in this Tender, the SI shall carefully consider the solutions it proposes and explicitly mention the same in the technical proposal
- Wherever required, optical line amplifiers shall be installed on the same cable at the appropriate distances considering the line losses.
- Cable loops are to be provided for future maintenance purposes at regular spacing.
- The ring will interconnect all the PoP substations with DCC and DRC. There shall be more than one ring.
- This ring will carry all the traffic from each districts to the DCC as well as each district to district. The core ring shall be designed to drop approx. 100 Gbps traffic in the ring and must factor in this 30% expansion for future bandwidth/port consumption.

Detailed Engineering (Design) & Documentation:

- Prepare detailed engineering drawings, installation methodologies, and a final Bill of Quantities (BoQ) for approval.
- The bidder should prepare propose the detailed survey report as per the Implementation Plan for the initial freezing of BOQ (as per actual Existing and Under construction Substations)

and Key considerations for the Integration with existing Distribution SAS substations.

- Develop core documentation: Functional Requirement Specification (FRS), System Requirements Specifications (SRS), High-Level Design (HLD), and Low-Level Design (LLD).
- Submit all surveyed route data, configuration plans, and design documents (HLD/LLD) to the central NOC repository for NEA review and approval.

b) Supply, Installation, and Commissioning

Fiber Optic:

- Supply, store, insure, transport, and deliver all ADSS fiber, accessories (FODBs, suspension/dead-end assemblies), and jointing equipment to site warehouses.
- Establishment of the Core Rings, Aggregation Rings, Pre-Aggregation Rings and Spur Connectivity including DWDM devices, Core Routers, DC PE Router, AGGREGATION Router, Region AGGREGATION Router, Core IGW Router, Network Management System of National Backbone Network for DWDM network including dedicated power backup and as per the final design duly approved by NEA.
- Utilize and integrate with existing OPGW cable runs by splicing ADSS fiber from the OPGW termination point to the respective substation/DCS/PoP location where DWDM is housed.
- Termination & Splicing: Perform all fiber splicing, termination (FODPs, joint boxes), and installation of splice enclosures. Install underground approach cable in substations and wherever aerial laying is not feasible.
- Coordinate with NEA authorities (Substation, LDC, DCS, PMD, DCC, DRC) and local government institutions for site access, route permissions, shutdowns, and necessary restorations.

SCADA System:

- Supply and install, configure and end to end testing of Remote Terminal Units (RTUs), LDMS (Local Distribution Management System), transducers, and communication gateways (OTN/GPRS) at all existing and upcoming substations.
- Install and configure OTN devices for SCADA data transmission where fiber to be laid under this project. Install and configure GPRS modems at all SS as secondary communication devices.
- Supply, install, and commission all SCADA software and hardware at the Distribution Command Centre (DCC) at Syuchatar and Backup Control Centre (BCC)/DRC at New Butwal with NOC.
- Integrate the Distribution Substation Automation System (SAS), with Load Dispatch Centre, LDC Backup, between DCC and BCC, 6 Grid MCCs, with current SCADA for KTM Valley at SS, upcoming GIS, DMS, OMS applications, existing/upcoming FRTUs/RTUs, wherever applicable.

Telecom Backbone:

- Supply and install new OTN devices at all Distribution Substations and augment/replace existing SDH equipment with OTN devices at Grid Substations to form the redundant OT Ring.
- Deploy DWDM systems, Optical Line Amplifiers (OLA), routers (Core, Aggregation, PE, IGW), and the Network Management System (NMS) for the IT Ring.
- Establish all Core and Aggregation PoP locations, including coordination of civil/electrical works to ensure suitable space and dedicated power backup for the terminal equipment.

Network Operations Centre (NOC) IT & OT Network:

- Setup two centralized Network Operation Centre to monitor the complete communication and SCADA network.
- Supply, installation, and configuration of servers, storage, networking, and security systems for NOC.
- Deployment of monitoring dashboards and analytics tools for network performance and event management.
- Integration of all network elements with the NOC for seamless management.
- NOC shall have a centralized monitoring console displaying network topology map. It shall provide key correlation analysis for network fault processing to improve network fault processing efficiency, provide performance & trend analysis of network equipment and impact range of network fault, network usage, availability and performance for server nodes. etc.

c) Testing & Commissioning

System Testing & Validation

- Conduct comprehensive Site Acceptance Tests (SAT) and Final Acceptance Tests (FAT) for SCADA, ADSS, OTN, and DWDM networks.
- Perform fiber testing for all laid links and submit reports (OTDR, insertion loss) in the appropriate format.
- Provide necessary testing equipment required to meet standards compliance for validation.

d) Documentation

- Submit all final documentation, including As-Built Drawings of SCADA Architecture, Communication, OTN & DWDM equipment topology, Fiber Route Maps, Network Configuration Records, and all System Documentation (FRS, HLD, LLD, manuals, SOPs, Change Management Histories).
- Provision a fiber health monitoring tool for the NMS to monitor fibers from Core to Spur/Joint Enclosure locations.

After completion of Works, final checking shall be done by the Contractor to ensure that all

Works, equipment erection etc. has been done according to specifications and as approved by the Employer.

e) **Operation & Maintenance:** This section details the contractual obligations for long-term support.
- **Maintenance Period (FMS/AMC):** The formal FMS/AMC/ATS period shall be for four (4) years, commencing from the date of issuance of the Operational Acceptance Certificate of the entire project.
- **Extended Warranty:** The Contractor shall secure and operationalize a minimum **five (5) year warranty** on all critical hardware (Servers, RTUs, Communication and Network Equipment) following Operational Acceptance.
- **Intervening Period O&M:** If any portion of the work is provisionally put into operation before formal Operational Acceptance, the Contractor shall be fully responsible for all support services, O&M, and defect rectification for that segment during this Intervening Period at no additional/extra cost to the Employer.
- **Service Level:** The SI must provide 24x7 support and maintain the deployed infrastructure in strict compliance with the defined Service Level Agreements (SLAs).

f) **Testing, Training, and Documentation**
- Testing: Conduct comprehensive FAT, SAT, and UAT for the integrated SCADA and communication networks in presence of NEA for validation and approval. All FAT logistics for NEA officials must be arranged and borne by the SI.
- Training: Provide extensive training programs both at the Manufacturer/Supplier's works (Foreign Training) and On-Job Training in Nepal for all technology domains, including SCADA Solutions, DWDM, OTN, and Fiber Network maintenance.
- Documentation: Submit all final documentation, including As-Built Drawings of SCADA Architecture, communication topology, and all design documents (FRS, HLD, LLD) for NEA's approval.
- SI shall conduct abroad training to the owner's employees as described in BOQ. All the expenses including training cost, airfare, hotel accommodation, food and incidental allowances (USD 150 per person per day) etc. shall be provided by the SI and has to include in proposed financial bid proposal.
- SI shall conduct local training in Nepal and all the training cost including trainer's charge, accommodation, and lunch for the trainees, training venue etc. has to be provided by SI and has to include in proposed financial bid proposal.

Additional Information:

- Any minor SCADA/communication equipment/items which are not mentioned in the bidding documents but are required for the successful completion of the project shall be in the scope of contractor for which no extra payment will be made and deemed to be included in the current price schedule.
- Any damages to the existing facilities of NEA and other utilities incurred by the Contractor during the construction process shall be borne by the contractor.
- NEA assumes that the SI is aware of any and all risks associated with this project and shall ensure all applicable safeguards. Under this assumption NEA considers itself indemnified

against any and all charges/legal proceedings for any accidents associated with the project.

3. Contract Execution Procedure

The contractor must submit a detailed project plan, outlining the timeline, resources, and methodologies to be deployed. Following approval of the project plan, the design phase commences, involving the creation of detailed architectural and engineering designs, which must be reviewed and approved by the client. SI shall start the procurement of the necessary hardware and software components after obtaining the approval of designs by the client. SI shall submit all the design documents according to the project plan. ensuring all supplies meet the specified technical requirements. During the installation phase, SI shall set up all the components of the project according to the approved designs. Throughout this phase, thorough testing shall be conducted to ensure functionality and compliance with project specifications. Subsequently, the commissioning phase involves the integration and testing of the entire system to verify operational readiness. This includes the configuration of the disaster recovery center, private cloud setup, and ensuring robust communication infrastructure for the data center and disaster recovery center as per the project plan timelines. Regularly, comprehensive trainings during installation, commissioning and UAT phases for client personnels should be provided to ensure effective management and operation of the newly installed systems. The project shall be ends up with a final review and acceptance by the client, ensuring all contractual obligations have been met satisfactorily.

4. Physical and other Parameters

Location of the Project Site: All provinces

5. Schedule of Quantities

The requirement of various items/equipment and work are indicated in Bid price Schedules. Wherever the quantities of items/works are indicated as a Lot, the bidder is required to quote price for entire execution and completion of works.

For erection hardware items, Bidders shall estimate the total requirement of the works and include the same in relevant Bid price schedules.

Bidder should include all such items in the bid proposal sheets, which are not specifically mentioned but are essential for the execution of the contract. Items which explicitly may not appear in various schedules and required for successful commissioning of this project (complete scope of work) **shall be included in the bid price bid and shall be provided at no extra cost to Employer**.

6. Reference Drawings

6.1 Basic general drawings are enclosed in the specification documents for reference, which shall be further engineered by the bidder.

6.2 In case of any discrepancy between the drawings and text of specification, the requirements of text shall prevail in general. However, the Bidder is advised to get these clarified from Employer.

7. Spares

Mandatory spares

The Mandatory Spares shall be included in the bid proposal by the bidder. The prices of these spares shall be given by the Bidder in the relevant schedule of BPS and shall be considered for evaluation of bid. It shall not be binding on the Employer to procure all of these mandatory spares.

The bidder is clarified that no mandatory spares shall be used during the commissioning of the equipment. Any spares required for commissioning purpose shall be arranged by the Contractor. The unutilized spares if any brought for commissioning purpose shall be taken back by the contractor.

8. Special Tools and Tackles

The bidder shall include in his proposal the deployment of all special tools and tackles required for operation and maintenance of equipment. The special tools and tackles shall only cover items which are specifically required for the equipment offered and are proprietary in nature. However, a list of all such devices should be indicated in the relevant schedule provided in the BPS. In addition to this the Contractor shall also furnish a list of special tools and tackles for the various equipment in a manner to be referred by the Employer during the operation of these equipment. The scope of special tools and tackles are to be decided during detail engineering and the list of special tools and tackles, if any shall be finalized.

9. Facilities to be provided by the Owner

The Employer may provide the auxiliary power supply from NEA on chargeable basis as temporary consumer. The prevailing energy rates shall be applicable. All further distribution from the same for construction and permanent auxiliary supply shall be made by the contractor. However, in case of failure of power due to any unavoidable circumstances, the contractor shall make his own necessary arrangements like diesel generator sets etc. at his own cost so that progress of work is not affected and Owner shall in no case be responsible for any delay in works because of non-availability of power

10. Specific Requirement

The Bidders are advised to visit project site and acquaint themselves with the topography, infrastructure, etc.

The bidder shall be responsible for safety of human and equipment during the working. It will be the responsibility of the Contractor to co-ordinate and obtain Electrical Inspector's clearance

before commissioning. Any additional items, modification due to observation of such statutory authorities shall be provided by the Contractor at no extra cost to the Employer.

The Contractor shall arrange all T&P (such as necessary supports, cranes, ladders, platforms etc.) for erection, testing & commissioning of the system at his own cost. Further, all consumables, wastage and damages shall be to the account of contractor.

The Contractor shall impart the necessary training to Employer's Personnel as mentioned in the RFP.

11. Pre commissioning, commissioning, Trial-Run & Completion

Pre-commissioning phase involves several critical activities to ensure a smooth transition to the subsequent stages: - a comprehensive project plan, detailed bill of material, detailed procurement plan including the timeline, milestones, resource allocation, and risk management strategies shall be submitted for approval. If SI shall implement the equipment / solutions without getting approval of the design and the implementation documents no payments will be processed for the solution.

Detailed design documents will be created, covering architectural, structural, electrical, and network designs, The same shall be reviewed and approved by the client. In the procurement stage, all required hardware, software, and materials will be sourced according to the tender technical specifications without any deviations. Site preparation is also a crucial part of this phase, involving any necessary construction or modifications to existing infrastructure.

The commissioning phase includes detailed design, procurement, installation, testing, and commissioning of all necessary components. Key deliverables include but are not limited to redundant power supply systems, high-speed communication links, robust network architecture, scalable storage solutions, and comprehensive disaster recovery drills. The selected vendor must demonstrate expertise in deploying secure and resilient IT infrastructure, ensuring seamless integration with existing systems, and providing ongoing support post-implementation.
Trail run activities focus on validating the functionality and readiness of the project under controlled conditions.

Upon completion of the project, several critical activities ensure its readiness and functionality. These include finalizing all installations and configurations of hardware, software, and networking components according to design specifications. Comprehensive testing will be conducted to validate the effectiveness of backup and recovery procedures, ensuring seamless data replication and continuity in case of disruptions. Documentation will be finalized, detailing all configurations, procedures, and test results for future reference and compliance purposes. Training sessions will be provided to staff members and relevant stakeholders on operating procedures.

12. Social Safeguard and Environment and Management Plan

The Contractor shall prepare Social Safeguard and Environment Management Plan to be implemented during execution of the Project. The following major activities shall be considered:

Labour recruitment: The Contractor shall give preference to the use of local and regional labour provided that it is consistent with the requirement of good workmanship based on the need of the project.

Staff training and sensitization: At the beginning of works the Contractor shall organize training and awareness-raising workshops intended for his teams to improve their understanding to prevent or minimize the impact of their activities on the environmental and social aspects to promote good relations with the local people.

Among other topics addressed should also include the following:

Likely environmental impact of works, good practices, preventive and corrective measures to be adopted; Rules and procedures for waste management at construction sites; Safety risks associated with the works, and preventive attitude to adopt; First aid and what to do in case of accident; General standards concerning relations with the local people; Risks and prevention of sexually transmitted diseases. The training and awareness sessions should be organized whenever new workers are recruited. Feedback and training during the works and after the monitoring and control exercise, additional training and awareness activities may be necessary if it happens that the previous sessions had failed to achieve the desired effects.

Demarcation, signing and closing of worksites: Setting up warning signs at worksites to limit the access of persons, machinery and equipment into construction areas and confine the works related to the construction process to the allocated areas.

Access to private property: Contractor shall coordinate with the Employer for the access of private property, if required. Crossing of private property shall be subject to prior notification to the owners and conducted in such a manner as to minimize damage to crops or other property on the land.

Discovery of relics of historical and archaeological importance: In the unlikely event of discovery of historical relics, the works will be interrupted temporarily and the discovery notified to the local authority responsible for cultural heritage in order to determine the appropriate course of action.

Restoration of sites: After the infrastructure has been put in place and the construction sites and equipment depots cleared, the sites should be rehabilitated without undue delay in the original condition or better, unless there are plans for future use requiring that such sites be left in their current state.

Storage and handling of hazardous substances: Hazardous substances such as oils, lubricants or other hazardous substances likely to contaminate surface or ground water and soil should be stored or handled in premises specially designed for this purpose, in order to protect the environment and human health. If the handling of oils and fuels is necessary, demarcated and waterproofed areas that may contain any spills must be provided.

Maintenance of equipment: Maintenance of equipment should not be performed immediately at the work site as far as practicable.

Air quality and noise pollution: Care must be taken to ensure that all equipment, machinery and vehicles used for works and equipped with a combustion engine are in good working conditions to limit undesired emission of air pollutants and nuisance.

Construction works that could cause noise should be performed only outside normal rest hours near residential areas. When noisy works must be carried out close to schools or other noise-sensitive receptors, working hours should be so scheduled as to limit the nuisance caused.

It is forbidden to burn in the open any kind of household, industrial and toxic or hazardous waste, project induced waste and all types of scrap metal.

Transportation of equipment: Equipment for overhead lines will be transported by existing roads up to the point nearest to the installation site. Thereafter, it will be transported manually to the site without opening up any access paths. When crossing the land between roads and installation sites, care should be taken not to damage vegetation, agricultural land or any other property on the land.

Erection of Poles: Vegetation should be removed only in so far as strictly necessary for opening foundations for poles and for such other operations as may be performed at each spot. When erecting the poles, necessary precaution should be taken to minimize the impact on adjacent areas.

Unrolling of cables: When cables are being unrolled, necessary precaution should be taken to prevent impact on tree vegetation, crops and other property on the land crossed by the cables. If necessary, temporary gantry-like structures should be used to facilitate crossings.

Restoration or damage compensation: If the works on private property cause damage to crops or other property, the Contractor must proceed with the repair of such damage or, where this solution is not sustainable, with the fair and timely compensation of the owners.

Management of material from digging trenches: Uncontaminated soil from excavations will be reused to backfill the trenches of underground lines. Any such soil that cannot be reused is deemed to be waste and must be conveyed to its final destination. Its uncontrolled spread is prohibited in places where it could cause damage. Minimum dust on ground policy is to be used to prevent dust associated pollution after the construction.

Sensitive Areas: From an environmental point of view, wetlands, swamps, and bogs should be avoided when planning underground cable as these habitats may suffer severe or even irreparable harm. Also sensitive water flows and archaeological sites should factor in route planning process.

Disruption of pedestrian and automobile traffic: When trenches are opened along the road, they should be barricaded, fenced off and warning signs placed at the worksites to ensure the safety of pedestrians, motorists and the staff carrying out the works.

There must be continued access to land and buildings located along trenches through installation of secure and clearly signalled temporary structures. This also applies to trenches that cut across the roadways.
Upon completion of the underground cable installation, the trenches should be resealed and the pavement repaired as soon as possible, to ensure its durability and the absence of irregularities that may present a traffic hazard.

Regular sprinkling of water shall be done to avoid dust pollution till the roads/sidewalks are reinstated.

Public information on electrical hazards, behaviour and preventive measures: Before switching on the infrastructure installed as part of the project, the neighbouring populations should be informed in good time, through public meetings and/or distribution of information leaflets. The information provided to them should focus on the electrical hazards associated with the infrastructure and the behaviour that would allow them to avert such hazards. The population of these areas should be particularly targeted.

Unanticipated Impacts identified during the construction should be mitigated in coordination with environmental and social monitors employed by Contractor, Consultant and Government separately.

13. Personnel Safety

The maximum safety consistent with good erection practices in the case of work above ground must be afforded to personnel directly engaged under this contract. Reasonable measures shall be taken to afford adequate protection against material falling from a higher level onto personnel below.

14. TRAININGS

The Contractor shall impart the necessary training to NEA's Personnel as per following details: -

1. **Training at Manufacturer/ Supplier's works:** The Contractor shall include in the training charges (i) Accommodation Charges (ii) payment of per Diem allowance to NEA trainees per day per trainee for the duration of training period abroad towards meals and other incidental expenses and (iii) to and fro economy class air ticket from Nepal to place of training. The duration of training shall be excluding travelling period. It shall be quoted under Schedule 4(b): Training Charges for training to be imparted abroad.

   The training shall be provided in the field of design, testing and maintenance at Manufacturer's works by OEM Certified Professional Training experts and the trainees should be provided professional level certifications.

2. **On Job Training in Nepal:** The traveling and living expenses of Owner's personnel for the training program conducted in Nepal shall be borne by the Owner. It shall be quoted under

Schedule 4(c): Training Charges imparted to Employer's Personnel by Bidder's Instructor in Nepal.

The training shall be provided to Employer's personnel in the field of erection, testing, operation and maintenance at substation sites respectively.

15. SERVICE LEVEL AGREEMENT (SLA)

Support services (including Maintenance) for 4 years:

After the successful commissioning of the entire project, the contractor shall provide the support services which shall include maintenance of the system installed under the project for a period of 4 (four) years from the date of issuance of operational acceptance of the project.

The Scope of Work shall includes SCADA solution (Software and hardware), LDMS, Fiber, IT & OT Ring (DWDM & OTN), NOC Infrastructure operation and maintenance support to be provided by the Contractor in respect of the system supplied under this project for a period of 7 years along with Supervision & Operation of the complete infrastructure along with communication network after the Operational Acceptance of the entire project. However during the execution of the infrastructure work it is expected that certain portion of the work if completed and put to service before the actual completion and commissioning of the entire project, then in that case also the support services including O&M shall be the responsibility of the contractor in accordance with this document, at no additional/ extra cost towards payment of support services (O&M) during this intervening period.

15.1 Single window service:

The Contractor shall provide a single window service to maintain SLA and in case of a joint bid only one organization shall be held responsible & accountable for the of the system as per defined SLA.

15.1.1 The bidder shall provide 24x7 support to NEA to comply with SLAs in case of any problem.

15.1.2 It shall be the responsibility of Contractor to resolve any related issues of SCADA, Fiber, IT & OT Ring system.

15.1.3 The Contractor is required to work with the Employer's technical personnel during whole SLA period. The Contractor shall support and build the capacities of local counterparts in the day- to day management, operation and maintenance of the network. Contractor shall conduct on the job training for these counterparts to ensure that they are able to maintain and operate the network in a stable and reliable manner in accordance with established Prudent Utility Practices.

15.1.4 The Contractor is required to provide field personnel for support service including Engineers, Supervisors etc. The numbers of field personnel shall be negotiated.

15.2**Scope of work includes but not limited to:**

15.2.1 Operation and running of the SCADA/Fiber/OTN/DWDM/NOC infrastructure etc.
15.2.2 Maintenance and Repair/ replacement of defective equipment under the project.
15.2.3 Predictive and preventive maintenance of the infrastructure.
15.2.4 Additions and deletions after the commissioning of the entire project is a dynamic phenomenon and shall be catered by the contractor. The network analysis with respect to the additions/ deletions in the OTN & DWDM network and designing of the network configuration shall also be carried out by the contractor.
15.2.5 Services to bring up any or all OTN & DWDM network upon its failure and to restore the functioning of the same etc.
15.2.6 Any future planning, estimation, augmentation and execution work for strengthening of the existing system shall be done by the contractor during the O&M period. Any material required for the above work shall be provided by the contractor on the same rates as per the award of original project.
15.2.7 On the Job Training for NEA's Staffs for operation and maintenance for equipment and system installed under the project.

15.3The cost for the SLA shall be deemed to be included in the cost of equipment in BPS.

16. Implementation Plan

The Contractor must adhere to the implementation plan as below:

Sr. No.	Activity Name	Timelines
1	**Acceptance of NoI/NOA, PBG Submission & Contract Signing**	**T*+1**
2	**Project Initiation Stage**	
a	Project Kick Off	**T+1**
b	Presentation on Execution Approach & Methodology to Senior Management	
c	Onsite Office Setup & Team Mobilization	
d	Requirement Analysis	
3	**Survey and Feasibility Study**	
a	GIS Survey of ADSS cable route and end end points	**T+6**
b	Site Survey (OTN)	
c	Site Survey (DWDM)	
d	Site Feasibility survey of Substations (SCADA)	
e	Compile findings in a comprehensive survey report.	
4	**Network Design, Architecture & Specification**	
a	Network Architecture Finalization	**T+6**
b	SCADA Solution Architecture finalization for substations	
c	General technical Particulars and GA drawing approval of Level1 & 2 Items	
d	Finalization of Technical Design Documents and approvals – HLD & LLD with layouts, schematics including communication network architecture & SCADA	
5	**Inspection, Procurement and MRHOV (Material receiving and Handing Over receipt Voucher)**	
a	Procurement Plan and Approvals	**T+8**
b	Factory Acceptance Test	
c	Pre dispatch inspection	
d	Procurement of Equipment and Materials	
e	Logistics and Material Distribution to site	
6	**Installation**	
a	ADSS Cable Implementation	**T+30**
b	OTN Solution Implementation	
c	DWDM Installation and Configuration	
d	Installation of SCADA Field Devices, S/w & H/w with Integration	
e	End to end testing & bug free operation: SCADA	
7	**Testing & Commissioning**	
a.	Testing of ADSS, OTN, DWDM, and SCADA systems.(overall)	**T+35**

b.	Testing of OTN	
c.	Testing of DWDM	
d.	Testing of SCADA	
e.	End to End testing of SCADA and telecommunication network	
8	**Operational Acceptance**	
a	Operational Acceptance after Commissioning	**T+36**
7	**AMC/ATS/FMS**	
a	AMC/ATS/FMS Services support for 4 (five) years post Go-Live including facility management and manpower deployment	**T+84**
8	**Training and Capacity Building**	
a	Continuous Training & handholding of Stakeholders.	**T+84**
9	**Performance Review & Project handover**	**T+84**

*** T- Contract Signing Date.**

17. Facilities to be provided by NEA

SI should submit an monthly shutdown plans in proper format for NEA to arrange necessary Power shutdowns across various sites.

----- End of Chapter 1 -----

CHAPTER 2: GENERAL REQUIREMENTS

a) General Requirements- OTN & DWDM (Part-A)

1. OTN Backbone Network (OT Network):

Substations have various services, including traditional SCADA, RTU, and relay protection services, traditional production services require stable, reliable, and low latency, new services such as AMI data backhaul, plant environment monitoring IOT, and security video surveillance services require certain bandwidth to meet service evolution requirements.

1.1 OTN System Design

In order to connect around each substation under the scope which are located in different cities and areas, a Backbone Interconnection Network is necessary. The OTN Backbone Interconnection Solution is compatible with current convergence and backbone network architecture and compliant with the trend of communication in the future. It is based on the OTN technology with high quality, high safety and low latency. It is a simplified and flat network with unified management and simplified maintenance. It can connect all the substations and dispatching center efficiently with high reliability and security.

Physical Layer

a) Wavelength range: 1260-1360 nm (O-band), 1530-1565 nm (C-band)

b) Fiber type: Single-mode fiber (SMF), Dispersion-shifted fiber (DSF)

Network Layer

a) Network architecture: Point-to-Point (P2P), Point-to-Multipoint (P2MP), Ring, Mesh

b) Topology: Linear, Ring, Mesh

c) Network protocol: SONET/SDH, Ethernet, MPLS-TP, OTN

d) Data rate: 10 Gbps, 40 Gbps, 100 Gbps

e) OTN hierarchy: OTU0 (1.25 Gbps), OTU1 (2.5 Gbps), OTU2 (10 Gbps), OTU3 (40 Gbps), OTU4 (100 Gbps)

Transmission Layer

a. Modulation format: Non-return-to-zero (NRZ), Quadrature Phase Shift Keying (QPSK), Quadrature Amplitude Modulation (QAM)
b. Forward Error Correction (FEC): Reed-Solomon, BCH, LDPC
c. Chromatic dispersion tolerance: ±1000 ps/nm
d. Polarization mode dispersion (PMD) tolerance: ±20 ps/km

Performance Specifications

a. Bit error rate (BER): 10^-12 to 10^-15
b. Error-free transmission: 99.999% (5-nines)
c. Latency: <10 ms (typical)

Interface Specifications

a. Optical interface: SC, LC, FC, MPO
b. Electrical interface: SFP, SFP+, XFP, QSFP
c. Ethernet interface: Gigabit Ethernet, 10GbE, 40GbE, 100GbE
d. SDH client interfaces: STM-1, STM-4, STM-16, STM-64
e. Network interface: OTU0, OTU1, OTU2, OTU3, OTU4

Standards and Compliance

a. ITU-T G.709: OTN framework
b. ITU-T G.872: OTN architecture
c. ITU-T G.957: OTN interfaces
d. IEEE 802.3: Ethernet standards
e. Telcordia GR-253-CORE: Network synchronization

Other Key Specifications

a) Power consumption: Varies by system
b) Operating temperature: -5°C to 50°C (23°F to 122°F)
c) Humidity: 5% to 85% (non-condensing)
d) MTBF (Mean Time Between Failures): 100,000 hours (typical)

OTN Equipment Specifications

e) Multiplexers: OTUk (k=0,1,2,3,4) multiplexers
f) Cross-connects: Optical, electrical, or hybrid
g) Amplifiers: Optical amplifiers (OAs), Erbium-doped fiber amplifiers (EDFAs)
h) Regenerators: 2R (re-amplification, re-shaping), 3R (2R + re-timing)

1.2 OTN Network Topology

The topology of the planned OTN backbone network is shown as below. It is consist of three

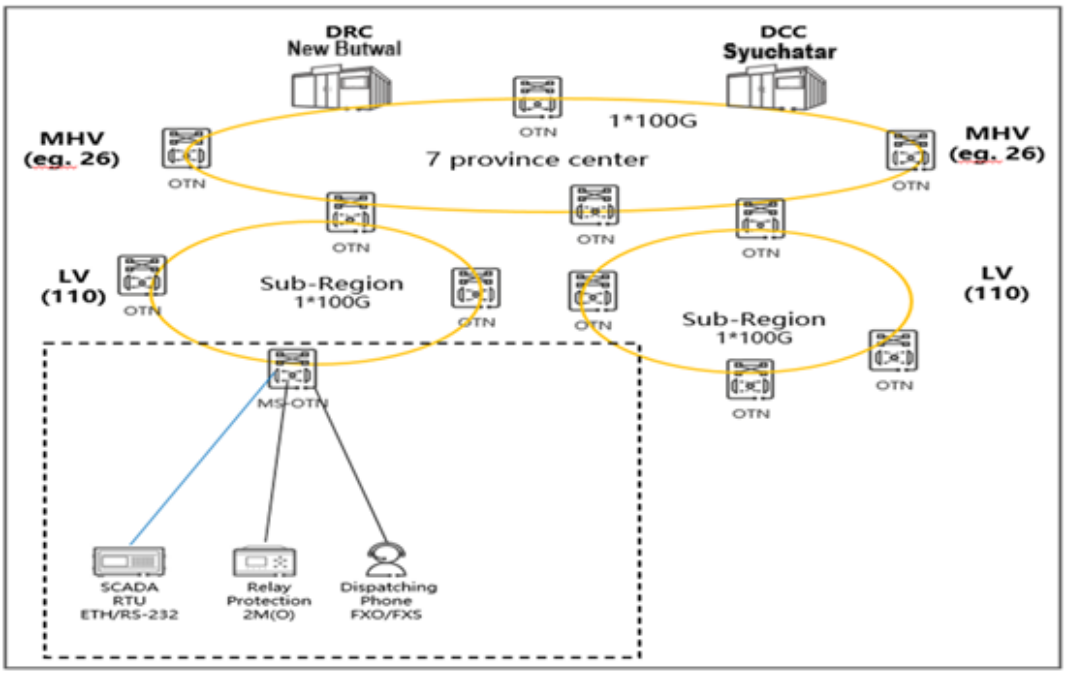
logical 100G OTU4 core ring and several access ring. OTN core 1 contain the main substations of the middle area of Nepal, such as Kathmandu Valley, the transmission rate is OTU4. OTN core 2 cover the North-west area main substations, the OTN core 3 cover the South-east area main substations, and the transmission rate is OTU4. Each one or two main substation will have 100G OTU4 access ring, each ring will connect the small substations. All of final plan and deployment will follow the actual site survey result and fiber resource condition.

The QTY of substation is shown below. In order to connect around 272 substations which are located in different cities and areas, a Backbone Interconnection OTN Network is necessary.

Table 2 : Quantity of Substations

Category	Description	Qty
Substation	Include 400/220/132/66KV substation	272
	Include 33/11KV substation	

Figure 2: Illustrative OTN backbone architecture



1.3 *Design of the substation*

a. Converter Substation

Converter Substation have Relay Protection system, Clock Synchronization system, Corporative Network, Operative Network, the main interfaces are FE/GE, E1.

The main service of Corporative Network are OA, video conferencing, administrative telephone.

The main service of Operative Network are Dispatch phone, CCTV, RTU (access control and environmental sensors), Engineering (EWS and RDP).

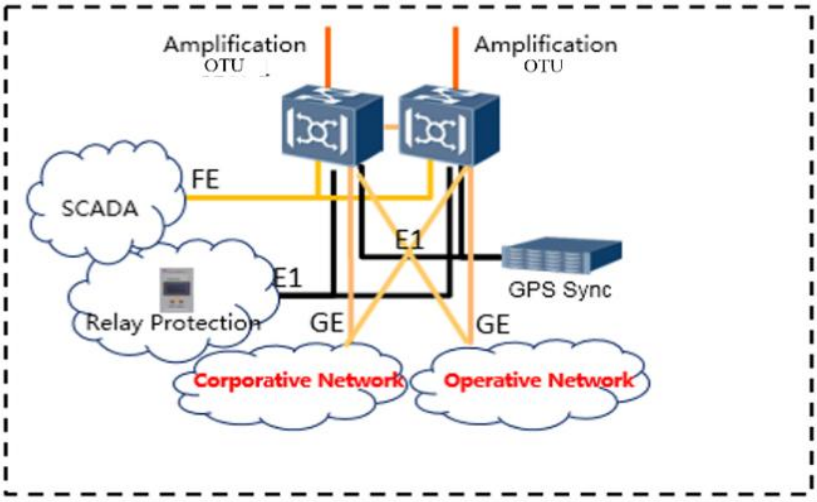


Figure 3: Illustrative Converter Substation architecture

b. Substation

Substations have Relay Protection system, Corporative Network, Operative Network, the main interfaces are FE/GE, E1.

The main service of Corporative Network are OA, administrative telephone.

The main service of Operative Network are Dispatch phone, CCTV, RTU (access control and environmental sensors), Network Management System and Engineering (EWS and RDP).

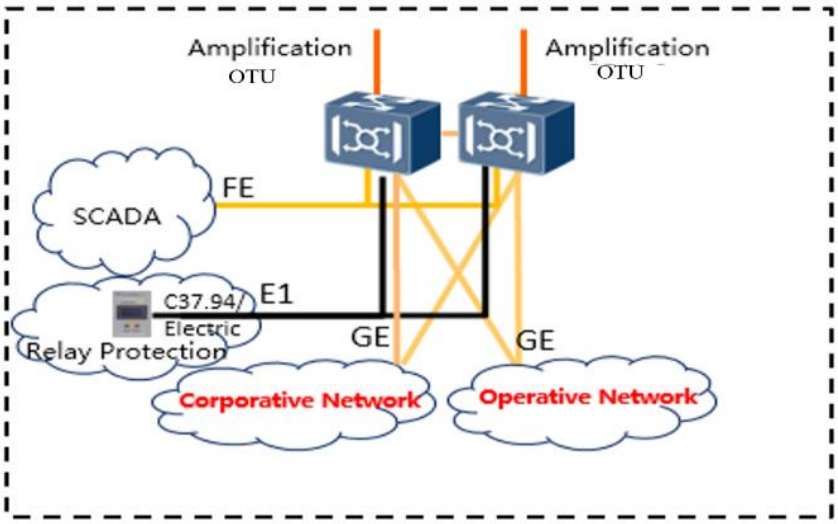


Figure 4: Illustrative Substation architecture

c. Repeater

Repeaters have Corporative Network and Operative network, the main interface is GE.

The main service of Corporative Network is administrative telephone.

The main service of Operative Network are CCTV, RTU (Oil engine, UPS, access control, air conditioner and environmental sensors) and Engineering (EWS and RDP).

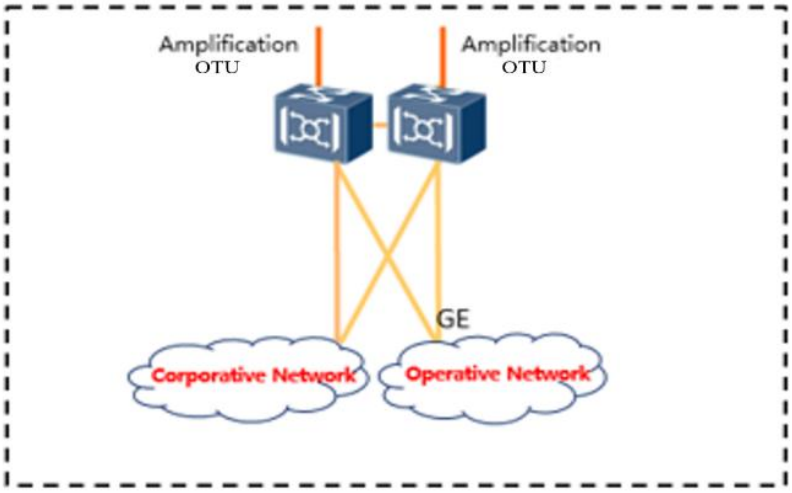


Figure 5: Illustrative Repeater architecture

1.4 *Interface of service Design*

d. Converter Substation

Network System	Service Type	Interface Type	Channel type
Line System	SSCL	FE/GE	Ethernet
Line System	PCP/LFL/SSCL	E1	SDH
Clock System	GPS	E1	SDH
Operative Network	SCADA/RTU/Voice	E1/FE	Ethernet
Corporative Network	Video Conference/ Voice/OA/CCTV	GE	Ethernet

Table 3: Interface for Converter Substations

e. Substation

Network System	Service Type	Interface Type	Channel Type
Line System	SSCL	FE/GE	Ethernet
Line System	PCP/LFL/SSCL	E1 Electrical E1	SDH
Operative Network	SCADA/RTU/Voice	E1/FE	Ethernet
Corporative Network	Video Conference/ Voice/OA/CCTV	GE	Ethernet
Protection	Optical 2M	Optical E1	SDH

Table 4: Interface for Substations

f. Repeater

Network System	Service Type	Interface Type	Channel Type
Line System	SSCL	FE/GE	Ethernet
Line System	PCP/LFL/SSCL	E1 Electrical E1	SDH
Operative Network	SCADA/RTU/Voice	E1/FE	Ethernet
Corporative Network	Video Conference/ Voice/OA/CCTV	GE	Ethernet

Table 5: Interface for Repeater

1.5 *Reliability design*

- **Network-Level Protection**

At the network level support Linear MSP, Ring MSP and SNCP network protections.

- **Equipment-Level Protection**

The equipment should support equipment-level protection, including switch and control 1+1 redundancy, secondary power supply module on the board, power redundancy, and fan redundancy.

Switch and control 1+1 redundancy. Switching 1+1 redundancy implements 1+1 protection for the SCC unit, cross-connect unit, and timing unit at the same time. The active and standby cross-connect units connect to service board slots through the backplane bus to protect cross-connection services.

Table 6 : Equipment Level Protections

Protected Objects	Description of protection
OTN	SNCP
Cross-connect and timing unit	1 + 1 Hot backup
SCC unit	1 + 1 Hot backup
The Power Interface Unit	1 + 1 Hot backup, 1: N centralized Backup
Intelligent Fan Unit	The power supply modules are of mutual backup for the three fan modules.
Board under abnormal conditions	Power-Down Protection During Software Loading, Overvoltage or Under voltage protection for power Supply and Board temperature detection

In order to connect around 272 substations which are located in different cities and areas, a Backbone Interconnection OTN Network is necessary.

Multi-Service Access.

The same device platform can support access Multiservice with different service cards be configured as per real onsite requirement: STM-N (1/4/16/64), E1/T1, E3/T3, FE/GE, STM-1/4 ATM, E3 ATM and Storage Area Network (SAN) like Ficon, FC and ESCON. Also, OADM and integrated PCM.

1.6 PCM should provide an all-in-one solution for low-speed service access

The transmission network carries various production and dispatching services. Different services should be accessed via different interfaces. The OTN equipment should access high-rate data services directly via E1/FE/GE interfaces. The OTN equipment should access a large number of low-rate services directly, including analog and digital signals (such as dispatching telephone

signals, office telephone signals, and monitoring, dispatching, and the measurement signals of production automation).

The solution's PCM components shall provide various low-rate interfaces and allow direct access of diversified production and dispatching services.

The multi-service access platform should support the following low-rate interfaces with different service cards: FXS, FXO, E&M, V.35/V.24/X.21/V.11/V.28, and RS232/422.

1.7 *Long distance inter-connect between cities.*

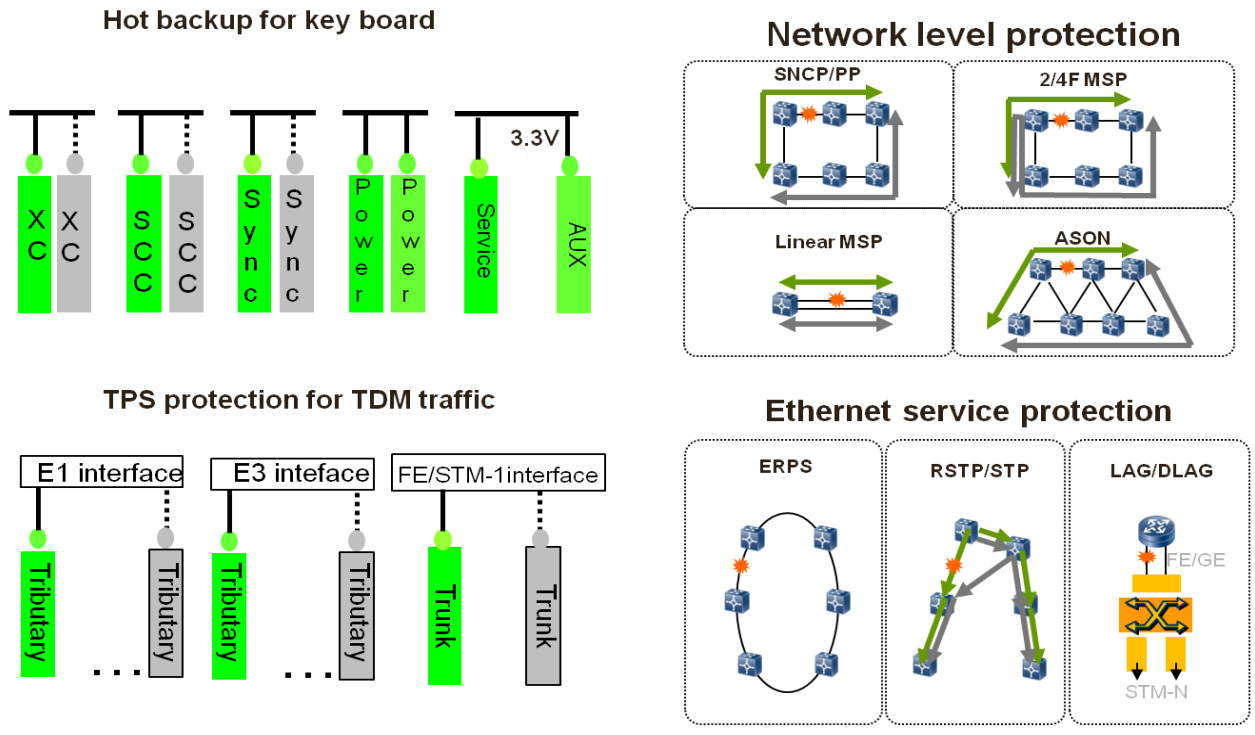
The OTN network can extend the one hop transmission distance from 80km to 200km, solve the transmit distance limitation of Switch and Router.

1.8 *Abundant and mature network level protection*

- **Abundant Network Protection Mechanisms**

The OTN network should provide a complete network protection mechanism.

Figure 5: Network Protection mechanisms



2. General Requirement of Network Management System for OT networks:

2.1 Topology Management

The NMS should has the Physical Root, Clock View, Tunnel View, and Custom View. These views provide easy access to important information, enabling user to ascertain and monitor the operating status of the entire network conveniently.

- **Topology view:**

The topology view of the NMS should consist of a navigation tree in the left pane and the Main Topology in the right pane. The navigation tree should show the network hierarchy and the Main Topology displays the objects at different coordinates on a background map, which helps identify the locations of deployed objects.

User can set the background of the Main Topology. The NMS should support pictures in .gif or .jpg format and provides many geographical maps for preferences.

- **Automatic discovery in the topology view:**

The NMS should provide an automatic topology-discovery function to automatically add NEs to the topology view. NEs (Network Element) can be created in batches. In addition, the NMS can automatically create fibers/cables and links.

- **Alarm display in the topology:**

In the topology view, alarms should be displayed in different colors or icons to indicate different status of the subnets and NEs. This function should allow user to monitor NE alarms in real time.

User can switch to the active alarm window of an NE using the shortcut menu of the NE node. In addition, user can query active alarm details

2.2 Alarm Management

If the network malfunctions, the NMS should troubleshoot network faults based on the alarm reporting and handling process.

The NMS should provide various visualized troubleshooting methods based on features such as service path visualization and masking of invalid alarm. When preprocessing alarms, user can use alarm templates to filter alarms on the NMS. After an alarm template is defined, the template can be used for multiple times to quickly find the desired alarm information. Alarms can be displayed on the NMS by alarm severity or alarm type. For example, different colors are used to distinguish alarms with different severities.

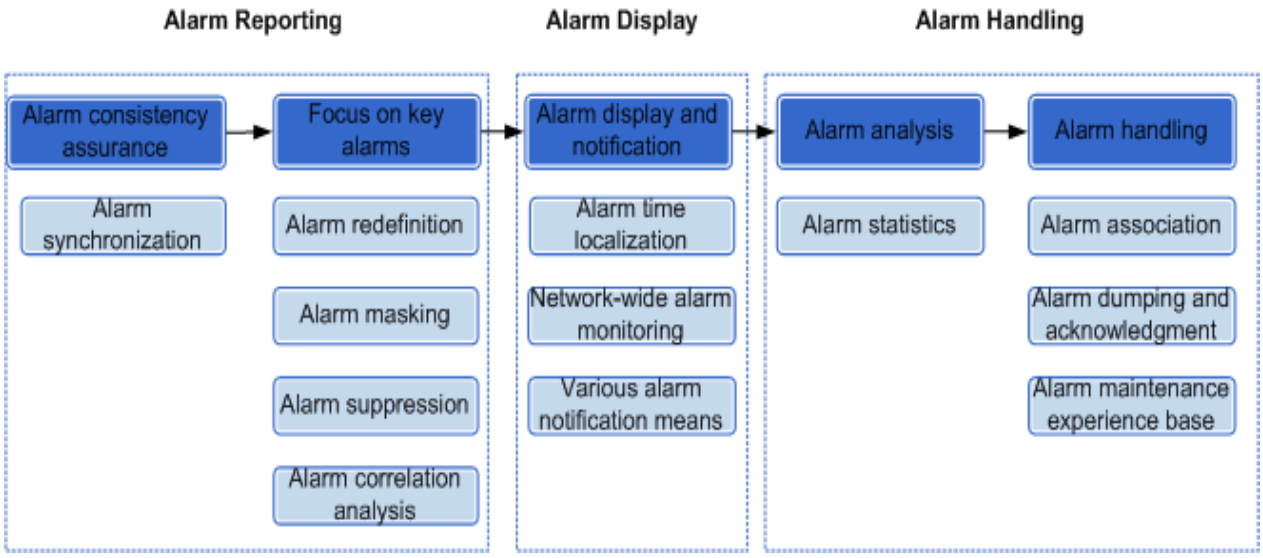


Figure: Alarm reporting and handling process

- **Alarm Filter and Display**

The NMS should distinguish root alarms from their correlative alarms and visualize the relationships between root alarms and correlative alarms within domains.

- **Alarm Correlation based on Service and correlation rules:**

Network alarms should be shown on topology nodes in less than 10 seconds. The alarm NBI to the OSS should support XML, SNMP, and CORBA protocols. NMS should automatically report network-wide alarms and display latest network conditions in real time, synchronizing alarm and events. The OSS can subscribe to or filter alarms and events or acknowledging and unacknowledging alarms and events. NMS can also report alarm correlation (alarm-affected services, paths, correlative alarms) change notifications.

2.3 Performance Management

The performance of a network may deteriorate because of internal or external factors and faults may occur. To achieve good network performance for live networks and future networks while controlling costs, network planning and monitoring are necessary. The NMS should implement 7x24 (24 hours per day for every week) performance management to help detect the deteriorating tendency in advance and solve the potential threats so that faults can be prevented.

The NMS should provide performance monitoring functions to support performance management at both the NE and network levels. By creating a performance instance, user can enable the NMS to collect performance data from network devices at specified intervals.

2.4 Inventory Management

The NMS should support unified inventory management of physical and service resources on the entire network. The NMS should provide clear and easily-accessible information to users so that they can acquire an accurate and complete understanding of the network-wide resources. The inventory information should serve as a reference for service and expansion planning.

Users can query inventory information, such as telecommunication rooms, racks, subracks, NEs, boards, sub boards, ports, slots, and links.

2.5 Security Management

NMS security should be ensured by user management, login management, rights- and domain-based management, and security policy management. Log management for user logins, user operations, and NMS running is used to enhance security management.

- **User Management**

The NMS should support user creation, modification, and deletion. The combination of a username and a password should uniquely identify the login, operation, and management rights of a user. User passwords are encrypted using the Advanced Encryption Standard (AES)-128 cipher and stored in a database.

The NMS should support user group creation, modification, and deletion. Five default user groups should be available: security management group, operator group, administrator group, guest group, and maintenance engineer group. The NMS should manage user rights using user groups, which reduces management costs.

- **Rights Management**

The NMS should support rights- and domain-based management. Only domain users with operation rights can perform operations on NEs. Using the right- and domain-based management function, users need to focus only on managed services. This eases key service monitoring and proactive operation and maintenance (O&M) and improves O&M efficiency.

The NMS should support menu item-specific operation rights.

IP domain: The NMS should support E2E service-specific management. E2E services include L3VPN, VPLS, PWE3 and aggregation services.

Transport domain: The NMS should support E2E service-specific management. E2E services include SDH and WDM services.

2.6 Service Provisioning and Assurance

NMS should provide end-to-end service provisioning and maintenance functions to the operators to improve the efficiency. And the smart diagnosis can be supported to tell the whether the fault is inside the OTN network or outside. And if it is inside the OTN network, NMS will tell the precise the faulty point to the operators.

- **End-to-end provisioning and maintenance:**

By using NMS end-to-end function, the operators just need to select the source, sink and the corresponding resource in the topology. NMS will calculate a shortest route automatically. In addition, operators just need to provision the OCH layer and the client layer. The other layers can be provisioned automatically by NMS.

And NMS should provide a centralized maintenance platform for OTN services. In the same interface, operators can get the signal flow, layers relationship, alarms displayed by layers, optical power, spectrum, bit error information.

- **Smart diagnosis:**

For OTN network, NMS should provide smart diagnosis functions. By initiating the smart diagnosis of a faulty path, NMS will check whether the fault is inside the OTN network or not. If the fault is inside the network, NMS will tell the precise fault point and generate test report.

- **Traffic-Aware Energy Efficiency**

The proposed equipment (Routers and DWDM) shall support intelligent energy-saving modes. The system must be capable of automatically putting unused ports, line cards, or optical components into a 'Sleep' or 'Low Power' state during periods of low traffic (dynamic power adjustment). This feature must be visualized and manageable via the NMS to support the NEA's green energy initiatives.

- **GIS-Integrated Fiber Health Monitoring:**

The built-in OTDR functionality shall be integrated with a Geographical Information System (GIS) map within the NMS. When a fiber cut or degradation is detected, the NMS must display the physical location of the fault on the GIS map (latitude/longitude) to guide field teams directly to the site, reducing Mean Time To Repair (MTTR).

3. General Requirement of IT Network - DWDM backbone:

3.1 DWDM Requirements:

The technical requirements of Optical Fiber Platform of Dense Wavelength Division Multiplexing (DWDM) technology (DWDM equipment) on single mode optical fibers conforming to ITU Rec. G. 652D. The key requirement is to transmit bandwidth efficiently that can be achieved with WDM deployments, considering the future expansion, the device capability can support following requirements with different service cards:

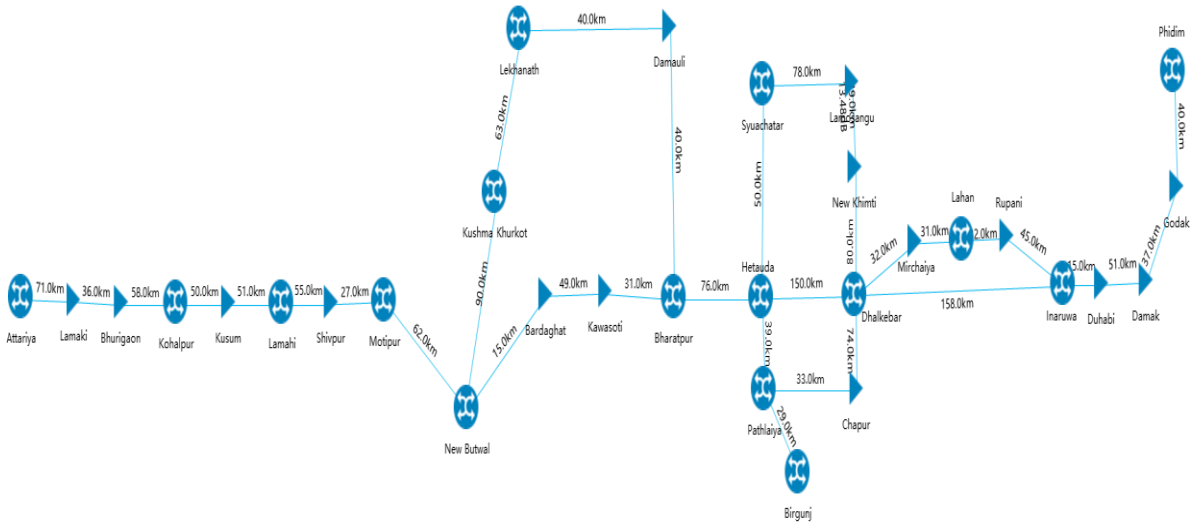
- Wavelength range: 1525-1572 nm (C-Band), 1575-1625 nm (L-Band)
- Channel spacing: 50 GHz, 100 GHz, 200 GHz, or flexible (Flexgrid)
- Wavelength tolerance: ±0.200 nm
- High capacity transport, At least 120@50GHz or higher OCh Mux/Demux.
- GE /10GE /100GE/STM4/STM16/STM64/FC800/FC1600/FC3200 Multiplexing and grooming capabilities, End to End transparency.
- Line side data rate: 100 Gbps, 200 Gbps, 400 Gbps, 600 Gbps, 800 Gbps
- Without requirement of any Regeneration of line signal (Minimum 100G per lamda) in between Source and destination node (Anywhere in between the Main, Protection and restoration paths).
- Modulation format: Quadrature Phase Shift Keying (QPSK), Quadrature Amplitude Modulation (QAM)
- Bit error rate (BER): 10^-12 to 10^-15
- Error-free transmission: 99.999% (5-nines)
- Without requirement of using any Dispersion Compensation module.
- Capable of implementing Protection and Restoration mechanism using Electrical ASON/GMPLS/Optical ASON for increased service availability and decreased downtime.
- Having inbuilt OTDR functionality.
- Required no. of WSS (9 Port or higher), Amplifier, OSC, OPS etc. equipped in optical sub-racks.
- All sub-Rack must have power and controller redundancy.
- OTN switch (If used) must have redundancy.
- Line and Client ports must be on separate cards.
- The offered DWDM equipment must be equipped in one equipment rack with all necessary hardware and software with license to provide line side protection and restoration facility (if fiber link available) through fiber connectivity.
- ITU-T G.694.1: DWDM wavelength grid
- ITU-T G.959.1: DWDM system requirements
- IEEE 802.3: Ethernet standards
- Telcordia GR-253-CORE: Network synchronization.

3.1.1 Design principles

In DWDM network, the transmission distance is mainly constrained by attenuation, OSNR (optical signal-noise-ratio) and dispersion.

3.1.2 Network Structure

As the below structure, the network includes OTM/OADM sites and OLA sites, OTM/OADM sites have service adding and dropping, OLA sites amplify the optical signals.



3.1.3 Network Fiber Loss

The standard attenuation coefficient is 0.275 dB/km for OPGW and ADSS optical cable, and the formula is 0.275*distance because the coefficient already includes other fiber factors.

3.1.4 Network Service Matrix

The integrated network Aggregationregates all signals from router, the services will depend on the bandwidth from each office branch and DC.

S.No.	Sites	New Butwal	Syuachatar
1	Attariya	1*100Ge	1*100Ge
2	Bharatpur	1*100Ge	1*100Ge
3	Birgunj	1*100Ge	1*100Ge
4	Dhalkebar	1*100Ge	1*100Ge
5	Inaruwa	1*100Ge	1*100Ge

6	Kohalpur	1*100Ge	1*100Ge
7	Kushma Khurkot	1*100Ge	1*100Ge
8	Lahan	1*100Ge	1*100Ge
9	Lamahi	1*100Ge	1*100Ge
10	Lekhanath	1*100Ge	1*100Ge
11	Motipur	1*100Ge	1*100Ge
12	New Butwal		4*100Ge
13	Phidim	1*100Ge	1*100Ge

3.1.5 Interface of service

The DWDM backbone network will bear the service from backbone Router considering future expansion, the interface between Router shall has capability to extend to 10GE /25GE /40GE/ 100GE/ 400GE.

3.1.6 Reliability design

Equipment-Level Protection

The equipment should provide equipment-level protection, including switch and control 1+1 redundancy, secondary power supply module on the board, power redundancy, and fan redundancy.

Switch and control card 1+1 redundancy. The active and standby cross-connect units connect to service board slots through the backplane bus to protect cross-connection services.

Table 3: Equipment-Level Protection

Protected objects	Description of protection
Cross-connect and timing unit	1 + 1 Hot backup
SCC unit	1 + 1 Hot backup
The Power Interface Unit	1 + 1 Hot backup, 1: N centralized Backup
Intelligent Fan Unit	The power supply modules are of mutual backup for the three fan modules.

Protected objects	Description of protection
Board under abnormal conditions	Power-Down Protection During Software Loading, Overvoltage or Under voltage protection for power Supply and Board temperature detection

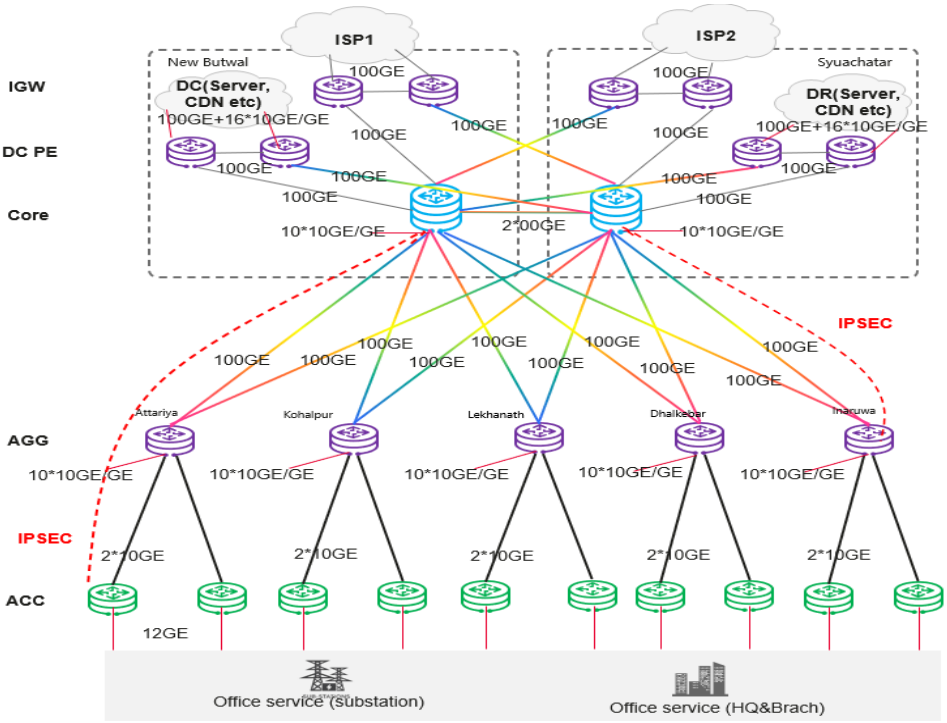
3.2 IT Network Solution for Office Services

3.2.1 IT Backbone Overview

Form the requirement for connect all office, NEA need to build an IT backbone network for office interconnected and have the service for internet.

Category	Description	Quantity
Access site	Egress router for office site	129
Aggregation Site	Aggregation Site	14
National Core	National Core Sites	2
DC	DC-PE	4
IGW	Core IGW	4

Each Access router from office connect to aggregation router with 2*10GE bandwidth for uplink. And for Aggregation device, 100GE link will be purposed to connect to national core router via DWDM device. All Access, Aggregation and Core router should support IPSEC for data encryption.



For internet connection, NEA can rent enterprise VPN form carrier, carrier provide a public IP address for NEA internet connection, all the BRAS function and NAT function will provide by carrier. And for NEA network, need to deploy 2 pair of IGW Routers to ISPs for internet connection. Based on above network model:

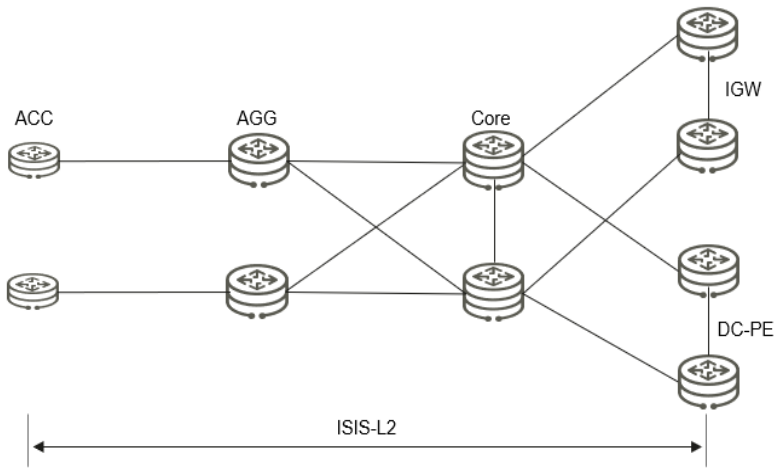
- One unified IP bearer network for all kinds of services;

- E2E network management, service provisioning and troubleshooting;
- Any connection, more flexible and faster network deployment.

3.2.2 Logical Network Design

3.2.2.1 IGP Design

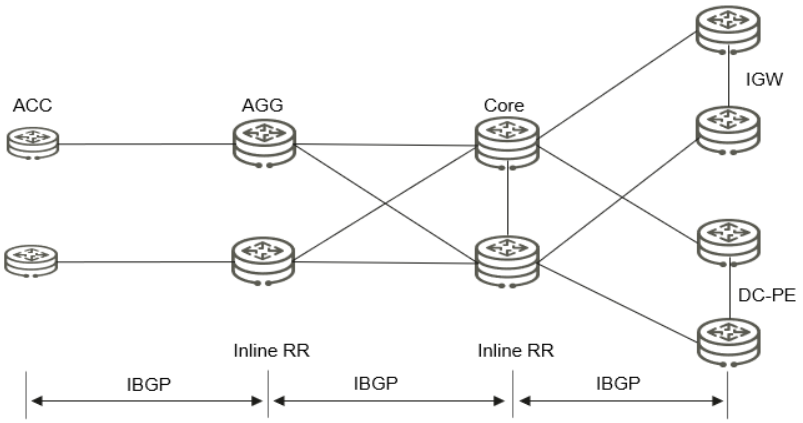
IGP is used for the connectivity within an AS (Autonomous System). ISIS and OSPF are the two most widely used IGP routing protocols. Both of them are link state routing protocols using Dijkstra algorithm, support level/area hierarchy for higher scalability, support fast convergence and fast reroute for high availability, and support IPv4/v6 routing and traffic engineering. For this project, suggest deploying ISIS as IGP so as to make it easier for future IPv6 evolution and network O&M. It is recommended to deploy ISIS level-2 in all routers.



The metric design will greatly affect the path selection. In other cases, the metric shall be specially designed. For example, for a network with dual plane topology, we can set the inter-plane link metric greater than the sum of intra-plane link metrics, so that we can ensure the traffic to be transported in the primary plane and be transported in backup plane after a switchover in case of any failure in the primary plane.

MD5 session validation, priority based fast convergence, NSF/NSR, IGP/LDP synchronization, BFD for IGP, OSPF, PRC, IGP FRR and etc. shall be enabled for security & resiliency.

3.2.2.2 BGP Design



- All backbone nodes are in the same autonomous system (AS). VPN route delivery via IBGP.
- Route reflectors (RR) could reduce the configuration complex and simplify BGP peers, it is recommended to deploy inline RRs on Core routers and AGGREGATION routers.
- Because VPN FRR protection is configured for the NEA network, RRs must be deployed in pairs for redundancy. An RR will select one from routes with the same route distinguisher (RD) and reflects the route to the clients. RRs need to be configured with the same cluster ID. All backbone nodes need to maintain the neighbour relationship with the two RRs and function as the RR clients. MED (recommended) values of the Local-preference values are used to determine the active/standby relationship.

3.2.2.3 Tunnel Design

LDP & RSVP are the two most widely used MPLS signaling protocols. LDP is short for label distribution protocol, and it relies on IGP for topology discovery and path selection. LDP is very scalable and suitable for small or large scale networks. RSVP relies on IGP for topology and link information discovery, then it can do best path selection based on the combination of different constraints, including link bandwidth, link color, SRLG and etc.

Future networks will be cloud oriented. Transport networks also need to be adapted to this and face the trends in simplifying networks, providing low latency, and implementing software-defined networking (SDN). Segment Routing MPLS or Segment Routing IPv6 (SRv6) is a protocol designed to forward IPv6/IPv4 data packets on a network using the source routing model. The network should be SR MPLS and SRv6 ready.

3.2.2.4 QOS Design

Detailed QoS processing are presented as below:

Processing on the ingress PE router:

The ingress LER of the MPLS domain limits the rate of the user data traffic using Committed Access

Rate (CAR) or other techniques to ensure the data flow complies with the bandwidth agreement of the MPLS domain. At the same time, it marks IP packets with different precedence according to the policy.

The length of the IP precedence field and that of the EXP field are both 3bits, and so the one-to-one mapping between IP precedence and EXPs can be conveniently made. In the Diff-Serv domain, the length of the IP DSCP field is 6 bits long, different from that of the EXP field, and so the many-to-one mapping between DSCPs and EXPs occurs. In the standard implementation, mapping is made between the first 3 bits of the DSCP (that is, CSCP) and the EXP, ignoring the last 3 bits in the DSCP.

Processing on the P router:

In performing MPLS label forwarding, the interior router in the MPLS domain (that is, LSR) executes various queues scheduling according to the information contained in the EXP field of the label of the received packet. In this way, the packet with higher priority is better served.

Processing on the egress PE router:

The egress LER in the MPLS domain needs to map the EXP field to the DSCP field of the IP packet. The standard mapping is the first three bits of the DSCP takes the EXP value and the last three bits takes the value of 0.

4. Network Management System (NMS) for DWDM & IT Backbone Networks

4.1 Topology Management

- The NMS should has the Physical Root, Clock View, Tunnel View, and Custom View. These views provide easy access to important information, enabling user to ascertain and monitor the operating status of the entire network conveniently.
- It is required that DWDM and IP router are managed by one NMS platform.

Topology view:

The topology view of the NMS should consist of a navigation tree in the left pane and the Main Topology in the right pane. The navigation tree should show the network hierarchy and the Main Topology displays the objects at different coordinates on a background map, which helps identify the locations of deployed objects.

User can set the background of the Main Topology. The NMS should support pictures in .gif or .jpg format and provides many geographical maps for preferences.

Automatic discovery in the topology view:

The NMS should provide an automatic topology-discovery function to automatically add NEs to the topology view. NEs (Network Element) can be created in batches. In addition, the NMS can automatically create fibers/cables and links.

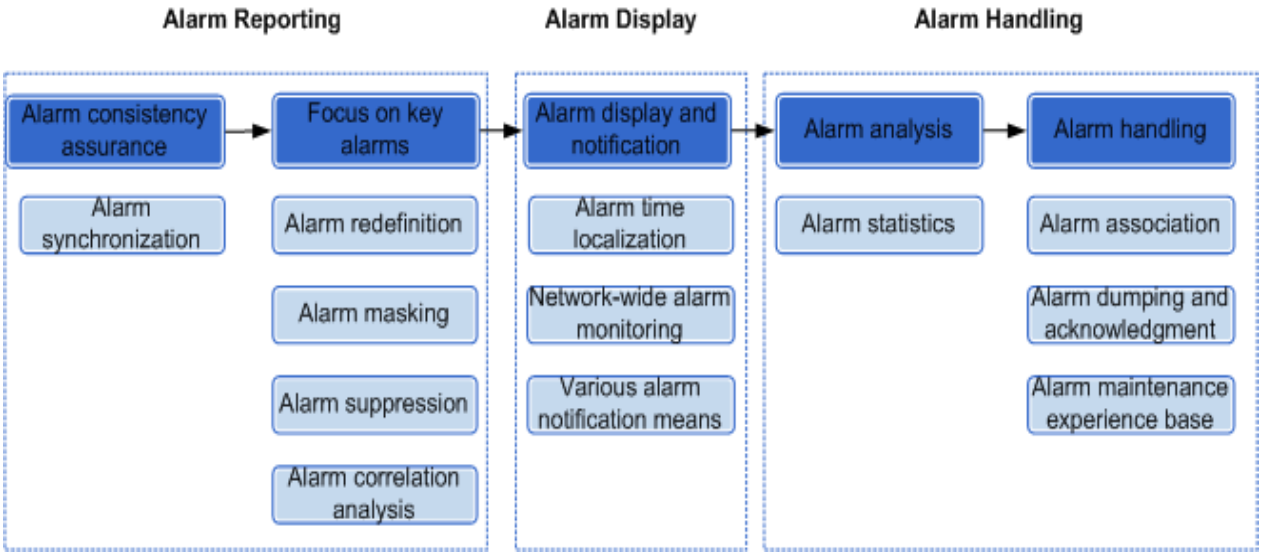
Alarm display in the topology:

In the topology view, alarms should be displayed in different colors or icons to indicate different status of the subnets and NEs. This function should allow user to monitor NE alarms in real time.

User can switch to the active alarm window of an NE using the shortcut menu of the NE node. In addition, user can query active alarm details.

4.2 Alarm Management

If the network malfunctions, the NMS should troubleshoot network faults based on the alarm reporting and handling process.



The NMS should provide various visualized troubleshooting methods based on features such as service path visualization and masking of invalid alarm. When preprocessing alarms, user can use alarm templates to filter alarms on the NMS. After an alarm template is defined, the template can be used for multiple times to quickly find the desired alarm information. Alarms can be displayed on the NMS by alarm severity or alarm type. For example, different colors are used to distinguish alarms with different severities.

Alarm Filter and Display

The NMS should distinguish root alarms from their correlative alarms and visualize the relationships between root alarms and correlative alarms within domains.

Alarm Correlation based on Service and correlation rules:

Network alarms should be shown on topology nodes in less than 10 seconds. The alarm NBI to the OSS should support XML, SNMP, and CORBA protocols. NMS should automatically report network-wide alarms and display latest network conditions in real time, synchronizing alarm and events. The OSS can subscribe to or filter alarms and events, or acknowledging and unacknowledging alarms and events. NMS can also report alarm correlation (alarm-affected services, paths, correlative alarms) change notifications.

4.3 Performance Management

The performance of a network may deteriorate because of internal or external factors and faults may occur. To achieve good network performance for live networks and future networks while controlling costs, network planning and monitoring are necessary. The NMS should implement

7x24 (24 hours per day for every week) performance management to help detect the deteriorating tendency in advance and solve the potential threats so that faults can be prevented.

The NMS should provide performance monitoring functions to support performance management at both the NE and network levels. By creating a performance instance, user can enable the NMS to collect performance data from network devices at specified intervals.

4.4 Inventory Management

The NMS should support unified inventory management of physical and service resources on the entire network. The NMS should provide clear and easily-accessible information to users so that they can acquire an accurate and complete understanding of the network-wide resources. The inventory information should serve as a reference for service and expansion planning.

Users can query inventory information, such as telecommunication rooms, racks, subracks, NEs, boards, sub boards, ports, slots, and links.

4.5 Security Management

NMS security should be ensured by user management, login management, rights- and domain-based management, and security policy management. Log management for user logins, user operations, and NMS running is used to enhance security management.

User Management

The NMS should support user creation, modification, and deletion. The combination of a user name and a password should uniquely identify the login, operation, and management rights of a user. User passwords are encrypted using the Advanced Encryption Standard (AES)-128 cipher and stored in a database.

The NMS should support user group creation, modification, and deletion. Five default user groups should be available: security management group, operator group, administrator group, guest group, and maintenance engineer group. The NMS should manage user rights using user groups, which reduces management costs.

Rights Management

The NMS should support rights- and domain-based management. Only domain users with operation rights can perform operations on NEs. Using the right- and domain-based management function, users need to focus only on managed services. This eases key service monitoring and proactive operation and maintenance (O&M) and improves O&M efficiency.

The NMS should support menu item-specific operation rights.

IP domain: The NMS should support E2E service-specific management. E2E services include L3VPN, VPLS, PWE3 and Aggregationregation services.

Transport domain: The NMS should support E2E service-specific management. E2E services include SDH and WDM services.

4.6 Service Provisioning and Assurance

NMS should provide end-to-end service provisioning and maintenance functions to the operators to improve the efficiency. And the smart diagnosis can be supported to tell the whether the fault is inside the OTN network or outside. And if it is inside the OTN network, NMS will tell the precise the faulty point to the operators.

End-to-end provisioning and maintenance:

By using NMS end-to-end function, the operators just need to select the source, sink and the corresponding resource in the topology. NMS will calculate a shortest route automatically. In addition, operators just need to provision the OCH layer and the client layer. The other layers can be provisioned automatically by NMS.

And NMS should provide a centralized maintenance platform for OTN services. In the same interface, operators can get the signal flow, layers relationship, alarms displayed by layers, optical power, spectrum, bit error information.

b) General Requirements- SCADA Solution (Part-B)

Nepal Electricity Authority (NEA) envisions the deployment of an advanced SCADA (Supervisory Control and Data Acquisition) system to enhance operational efficiency, reliability, and centralized control across its power distribution network. The project scope includes integration of RTUs (Remote Terminal Units) substations, supporting IEC 61850-compliant devices for bay-level I/O coverage, and ensuring backward compatibility with existing infrastructure.

The SCADA system implementation will encompass the end-to-end lifecycle of activities including site survey, detailed engineering and design, procurement, supply, installation, testing, commissioning, operational acceptance, and go-live, along with a Service Level Agreement (SLA) for post-deployment Facility Management Services (FMS) for a period of 4 years.

The System Integrator (SI) shall be responsible for establishing the SCADA Control Center (DCC), Backup Control Center (BCC), dispatcher training simulator (DTS), load shedding applications, and information storage and retrieval systems.

The system must ensure secure communication between substations and control centers using VPN/SSL over OTN fiber, GPRS/MPLS-4G/DLC networks, and support protocols like IEC 60870-5-104, DNP3.0, MODBUS RTU/TCP, IEC 61850, and ICCP (TASE.2).

Key hardware and software components include RTUs, multi-function transducers (MFTs), protection devices, servers, routers, switches, firewalls, storage systems, and communication equipment, all designed to be scalable for future network expansion.

The SI shall also be responsible for system integration with NEA's Load Dispatch Center (LDC), legacy SCADA systems, and other existing IT infrastructure using industry-standard protocols

and middleware. Comprehensive cybersecurity compliance in line with ISO/IEC 27001, IEC 62443, NIST CSF, and national standards shall be ensured through regular audits, vulnerability assessments, and threat mitigation.

Additionally, the SI shall manage complete testing processes including Factory Acceptance Tests (FAT), Site Acceptance Tests (SAT), and type tests, with defined performance benchmarks. Full documentation including system design, deployment architecture, engineering drawings, and operation manuals must be submitted and approved by NEA prior to deployment. The contractor shall also deliver extensive training for NEA's core implementation and operations teams and provide regular project progress updates.

Specific exclusions from the SI's scope include civil and architectural works, air conditioning, fire protection systems, and raw power supply, which will be provided by NEA based on the SI's space and utility requirements. The SCADA system shall come with a comprehensive four-year warranty post-operational acceptance, covering all supplied hardware and software components.

The contractor must ensure smooth transition to NEA's O&M team, provide spare inventory for the FMS period, and fully support integration, change management, and database/report

development throughout the system's lifecycle.

c) General Requirements- ADSS (Part-C)

The All Dielectric Self Supporting (ADSS) Fiber Optic Cable shall be designed and manufactured to provide reliable and durable performance under diverse environmental and operational conditions.

It shall be entirely non-metallic in construction, ensuring suitability for installation on 33kV/11kV lines, and optionally on LT lines, without risk of electrical conductivity. The cable must be robust, rigid, and capable of withstanding mechanical stresses such as impact, vibration, bending, and thermal aging throughout its operational lifecycle.

The cable shall be engineered for use in outdoor environments, including saline and corrosive atmospheres, and shall exhibit resistance to corrosion and degradation. The design life of the cable shall be a minimum of 25 years. The manufacturer must submit supporting statistical and test data, including cable aging test results, to substantiate the claimed lifespan of the fiber and all other integral components.

The ADSS cable and its associated hardware must conform to relevant TEC Generic Requirements, specifically TEC/GR/TX/OAF-001/03/MAR-17 (and its latest amendments) for accessories and fixtures. All required installation hardware, including fixtures for suspension, anchoring, and splice closure mounting on poles or towers, must be supplied as part of the complete system. The cable must also be fully compatible with the splice closures, which must comply with TEC/GR/TX/OJC-002/03/APR-2010 and amendments thereafter. The manufacturer shall specify the type, make, and model number of the splice closure to be supplied along with the cable.

The ADSS cable shall conform to the specifications of TEC GR No. TEC/GR/TX/OFC-022/02/MAR-17 Type III-A, or the latest applicable revision, and be suitable for the following operational conditions: a maximum span length of 100 meters, ice loading of 0 kg/m, and operational wind speeds up to 100 km/h. The allowable sag under normal conditions shall not

exceed 1% of the span length, and not more than 2% under excess load. The cable shall be operable in temperature ranges from -40°C to +70°C. It must be designed to endure a tensile force equivalent to $9.81 \times 4.0 \times W$ (where W is the weight of 1 km of the cable in kg), and must maintain a minimum bending radius of 10 times the outer diameter of the cable. Additionally, the cable must be installed maintaining a minimum clearance of 1.5 meters from any phase conductor on 33/11kV lines.

All components of the ADSS cable system must be designed to ensure safe, efficient, and long-term operation, while facilitating ease of installation, splicing, and maintenance.

----- End of Chapter 2 -----

CHAPTER 3: TECHNICAL REQUIREMENTS

1. Technical Specifications: OTN & DWDM (Part-A)

The capabilities of the offered equipment should comply with the detailed technical specifications in the condition of the additional required components (e.g. accessories, service boards, license, etc.).

1.1 OTN Network Solution for Substation

Detailed Technical Specifications and Standards [whenever necessary].

Item	Subject matter	Specification	Comply (Yes/ No)	Remarks
1	Technical Documentation	The Contractor shall provide technical information regarding the solution offered, presenting each of the equipment that will be part of the solution, as well as the Technology to be used. The technical documentation to be provided should cover all aspects relating to the Operation, maintenance, configuration and management of all equipment and systems Supply, as well as all documentation of all Provided.		
2	Standards and Recommendations	The proposed equipment must comply with the latest revisions of the Standards cited in this item		
3		High frequency disturbances (SWC) - Standards IEC 255-22-1 or IEC 1000-4-4- 1995-01;		
4		Disturbances by electrostatic discharge, - Standards IEC-255-22-2 or IEC 1000-4-2- 1995-01;		
5		Environmental conditions - Standard ETSI - EN 300 019-2-3 - Environmental Conditions and environmental tests for telecommunication equipment. Part 2-3:Specification of environmental tests - Stationary use at weather protected Locations;		
6		Ventilation and thermal performance of racks and sub-racks - ETSI standard - EN 300 119-5 - European telecommunication standard for equipment practice; Part 5 -Thermal management;		
7		Direct current supply - ETSI - Environment engineering (EE) standard; Power supply interface at the input to telecommunications equipment; Part 2: Operated by direct current (dc).		
8		Optical Safety: IEC 60825-1; IEC 60825-2;		

Item	Subject matter	Specification	Comply (Yes/ No)	Remarks
9		IEC 60825.1 Safety of Laser Product, Part 1: equipment classification, Requirements and user's guide		
10		IEC 60825.2: 2004 + A1: 2006 Safety of Laser Product, Part 2: Safety of optical fiber Communications systems (OFCS);		
11		The Electromagnetic Interference(EMI), Susceptibility(EMS) of equipment should comply with EN 55032, IEC 61000-6-5, IEEE 1613, IEC 61850-3, the bidder should provide the related test report.		
12		The bidding equipment should acquire the CC certificate issued by FIPS/NSCIB/BSI or the equivalent organization and provide corresponding report.		
13	Practices and Recommendations for OTN Equipment	G.652 Characteristics of a single-mode optical fiber and cable		
14		G.655 Characteristics of a non-zero dispersion-shifted single-mode optical fiber		
15		G.661 Definitions and test methods for the relevant generic parameters of optical Amplifier devices and subsystems		
16		G.662 Generic characteristics of optical amplifier devices and subsystems		
17		G.663 Application related aspects of optical amplifier devices and subsystems		
18		G.664 Optical safety procedures and requirements for optical transport system		
19		G. 665 Generic characteristics of Raman amplifiers and Raman amplified		
20		G.671 Transmission characteristics of optical components and subsystems		
21		G.691 Optical interfaces for single channel STM-64 and other SDH systems with Optical Amplifiers		
22		G. 692 Optical interfaces for multichannel systems with optical amplifiers		
23		G.693 Optical interfaces for intra-office systems		
24		G.694.1 Spectral Grids for WDM Applications: DWDM Frequency Grid;		
25		G.696.1 Infrasound compatible DWDM applications longitudinally		

Item	Subject matter	Specification	Comply (Yes/ No)	Remarks
26		G.697 Optical monitoring for DWDM systems		
27		G.698.2 Single channel optical channel amplified multichannel DWDM applications Interfaces		
28		G.703 - Physical / electrical characteristics of hierarchical digital interfaces		
29		G.707 - Network node interface for the synchronous digital hierarchy (SDH);		
30		G.709 / Y.1331 Interfaces for the Optical Transport Network (OTN)		
31		G.783 - Features of Synchronous Digital Hierarchy (SDH) Functional blocks;		
32		G.798 - Characteristics of the optical transport network hierarchy Functional Blocks		
33		G.803 - Transport-network architecture based on the digital synchronous system Hierarchy (SDH)		
34		G.805 Generic functional architecture of transport networks		
35		G.806 Characteristics of transport equipment - Methodology of description and Generic functionalities		
36		G.808.1 Generic protection switching - Linear and subnetting protection;		
37		G.825 - The control of fluctuation and drift in digital networks which are based In the synchronous digital hierarchy (SDH)		
38		G.841 - Types and characteristics of SDH network protection architectures		
39		G.870 / Y.1352 Terms and definitions for Optical Transport Networks (OTN)		
40		G.871 / Y.1301 Framework for the optical transport network Recommendations		
41		G.872 The functional architecture of optical transport networks using modelling Methodology described in G. 805;		
42		G.873.1 Optical Transport Network (OTN): Linear Protection		
43		G.874 Management aspects of optical transport network elements		
44		G.957 Optical interfaces for equipment and systems relating to the synchronous Digital hierarchy		
45		G.959.1 Optical transport network physical layer		

Item	Subject matter	Specification	Comply (Yes/ No)	Remarks
		interfaces		
46		G.7041 / Y.1303 Generic framing procedure (GFP)		
47		G.7042 / Y.1305 Link capacity adjustment scheme (LCAS) for virtual concatenated		
48		G.7710 / Y.1701 Common equipment management function requirements		
49		G.8201 Error performance parameters and objectives for multi-operator international paths within the Optical Transport Network (OTN);		
50		M.3010 Principles for a telecommunications management network		
51		IEEE 802.3 part 3: Carrier sense multiple access with collision detection (CSMA / CD) access method and physical layer specification		
52		IEEE 802.3ab - 1000Base-T - Twisted-pair Gigabit Ethernet		
53		IEEE 802.3a part 3: Carrier sense multiple access with collision detection (CSMA / CD) access method and physical layer specification. Amendment: media Access control (MAC) parameters, physical layers and management parameters For 10Gbps operation, 10 Gigabit Ethernet over fiber; 10GBase-SR (short reach), 10GBase-LR (long reach), 10GBase-ER (extended reach) and 10GBase-ZR;		
54		IEEE 802.3z Media Access Control (MAC) parameters, physical layer, repeater And management for 1000Mbps operation, 1000BaseX - Fiber Optic Gigabit Ethernet - 1000BaseSX (multimode) and 1000BaseLX (monomodal).		
55		IEEE 802.3x auto-negotiating full / half-duplex mode, automatic;		
56	System Architecture for OTN Equipment	To ensure high reliability for production services and efficiency for packet services, the offered system shall utilize a Universal Switching or Hybrid architecture. It must be capable of natively processing both ODUk (TDM) and Packet (MPLS-TP/Ethernet) traffic within the same sub-rack. The system shall guarantee strict bandwidth isolation (Hard Pipe technology or equivalent) for critical utility traffic, ensuring zero interference from bursty		

Item	Subject matter	Specification	Comply (Yes/ No)	Remarks
		Ethernet traffic.		
57		The offered OTN systems shall be the next generation systems and compatible with different types of data services (Ethernet, Fast Ethernet, Gigabit Ethernet, VLAN, etc.) other than PDH. These systems shall be able to provide EoS (Ethernet over SDH) and MPLS-TP service compliant with ITU-T G.7041, ITU-T G.783, ITU-T G.707 and ITU-T G.7042		
58	Equipment Capabilities	The proposed equipment shall support centralized universal switch, including Packet /ODUk switch plane in one equipment. The ability to flexible crossing of the systems shall be at least 900G ODUk and 900G packet capacity.		
59		To ensure comprehensive service access and efficient service grooming, the bidding system can access PCM, PDH, SDH, and ETH services. In addition, electrical-layer devices must support the OTN architecture, separate tributary boards and line boards, and unified PKT/VC/ODUk switching boards to facilitate smooth service upgrade and evolution.		
60		The offered OTN system shall transport with 100G OTU4 or higher rate in the line side for each direction.		
61		The proposed OTN equipment shall support STM1/4/16/64 interface.		
62		The proposed OTN equipment shall support FE/GE/10GE electrical/optical interface.		
63		The proposed OTN equipment support EPL/EVPL/EPLAN/EVPLAN L2 service.		
64		The proposed OTN equipment support 32*E1 card with TPS 1+1 protection.		
65		The offered OTN System shall be synchronized to a reference timing resource conforming to ITU-T G.811 quality. The OTN System shall perform the functionality described in ITU-T G.783 Recommendation as a timing source (SETS).		
66		The bidding equipment must support at least 100		

Item	Subject matter	Specification	Comply (Yes/ No)	Remarks
		kilometres transmission without electrical regeneration with successful case.		
67		The bidding systems should also support PCM service access and can be managed by one NMS system.		
68		The bidding equipment shall provide dispatching telephone, relay protection, and dispatching system service interfaces. Interfaces must support at least loop trunk interfaces (FXOs connected to switch subscriber lines). Subscriber line interface (FXS directly connected to a telephone) 2-wire audio interface; 4-wire audio interface; Two-wire EM interface; 4-wire EM interface; Asynchronous RS232/V.24 interface; Synchronous RS232; RS422 interface; RS485 port; V.35 interface (1-30 x 64 kbit/s bandwidth) G.703 64 kbit/s codirectional data interface.		
69		The bidding equipment shall support optical interfaces integrated according to the IEEE C37.94 specification. Supports link fault response and 2 Mbit/s optical transparent transmission.		
70		The proposed equipment shall support FXS/FXO service, and the same interface shall support setting to FXO or FXS through software		
71	Reliability	The proposed equipment supports LAG/LCAS/LPT/STP/RSTP/APS L2 protection.		
72		To avoid mis operation of the power relay protection device caused by network communication faults, the bidding equipment shall support the lossless switching function of the relay protection service to ensure the reliability of the power network. For service protection, the following conditions must be met: 1. At least two protection trails must be supported to provide protection against multiple (more than two) fiber cuts. 2. If the working path is interrupted or abnormal, protection switching is performed. Services are not interrupted, or bit errors occur.		

Item	Subject matter	Specification	Comply (Yes/ No)	Remarks
73		The power supply, control board, clock board, and cross connect board of the bidding equipment must be configured with 1+1 protection. For boards with hot backup, the active and standby boards can be forcibly switched over through the NMS, and the NMS screenshots must be provided for proof.		
74	Environment Requirements	Comply to ETSI Class 3.1 standard, the temperature range: Storage (ETS 300 019-1-1): –40°C ~ +70°C Transport (ETS 300 019-1-2): –40°C ~ +70°C Operation (ETS 300 019-1-3): Long-term operating temperature: -5°C to 50°C, Short-term operating temperature: -10°C to 55°C		
75		The bidding equipment must support both AC and DC Power Supply Modules. DC power input range Standard operating voltage: -48 V to -60 V Operating voltage range: -40 V to -72 V AC power input range Standard operating voltage: 100 V to 240 V Operating voltage range: 90 V to 264 V		

1.2 Network Management System of OT Network

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
1	Management System	The network management system must be the OEM's proprietary solution OR a commercially available third-party NMS that can provide full FCAPS (Fault, Configuration, Accounting, Performance, Security) management of the proposed router.		
2		The Management System and its respective hardware have a management capacity of at least 5 (five) times the final projected number of elements of the proposed network.		
3		The Network Management System to be deployed will also manage any of the network elements that are provided.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
4		The Management System allows the backup of all the configuration information of the network elements, so as to guarantee the maintenance of the operability of both the network and the management system, in any failure situation.		
5		The Management System makes it possible to download the configurations of the network elements, to perform their update in cases of failure and also to update the software of these elements in cases of system upgrade.		
6		The Management System must provide a clear separation of responsibilities between element-level configuration/monitoring and network-wide orchestration/service provisioning.		
7		All the configuration of the equipment is made through the management system, which should even allow the software update remotely, through specific commands.		
8		Access to each network element through the management system is protected by passwords in security level categories.		
9	SPECIFIC TECHNICAL REQUIREMENTS OF THE MANAGEMENT SYSTEM	NMS complies with the mainstream SDN architecture defined by Internet Engineering Task Force (IETF), generally consisting of Management/Orchestration and Control/Element layers.		
10		NMS is capable of full-service lifecycle management, capability exposure, and intensive, automated, and intelligent operation and maintenance (O&M).		
11		NMS provides unified user interfaces (UIs) for network management, control, and analysis.		
12		NMS can manage legacy devices. It manages and controls legacy networks and SDN networks in the same way.		
13		NMS provides a unified portal. All functions are available on this portal, and users do not need to open different systems.		
14		NMS complies with mainstream IETF and Abstraction and Control of Traffic Engineered Networks (ACTN) standards.		
15		NMS supports RESTful APIs and YANG models		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
		for programmability.		
16		NMS complies with the following YANG language standards: RFC 6991, RFC 7951, RFC 7950, and RFC 7895.		
17		Data transmission channels support secure protocols, such as Hypertext Transfer Protocol Secure (HTTPS), Simple Network Management Protocol Version 3 (SNMPv3), and Transport Layer Security (TLS).		
18		Web application firewall (WAFs) can be deployed to defend against SQL injection, cross-site scripting attacks, malicious code protection, and application-layer denial of service attacks.		
19		Data is transmitted on networks at the risk of being eavesdropped, tampered, or copied and resent. Controllers need to implement end-to-end (E2E) encryption on various interfaces.		
20		SSL/TLS protocol: supports the TLSv1.2 protocol released by IETF.		
21		Internal channels: use HTTPS to encrypt the data exchanged among management services (such as the installation, monitoring, upgrade, and maintenance services).		
22		Support Account policy: - Minimum number of characters in the account name - Max. number of inactive days - Lockout upon consecutive login failures - IP address range - Account lockout policy - Login time range - Max. consecutive failed login attempts - Account lockout duration (if not permanent) - Auto delete long locked or disabled accounts - Log out of unauthorized sessions		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
23		Support Password policy: - At least three types of characters (uppercase letters, lowercase letters, digits, and special characters) - Min. password length - Previous passwords disallowed - Max. times a character can occur - Min. interval between password change operations - Min. special characters - Enforce password expiration - Password validity period - Days of warnings prior to password expiration - Log out of the current session after password reset - Weak password dictionary		
24		Controllers can record complete logs about its own status, security events, operations, and configurations for query and audit, real-time check, analysis, and protection.		
25		System logs record abnormal status and actions when NMS is running, such as failure to execute scheduled tasks.		
26		The NMS uses different CA certificates for different peer systems (northbound, southbound, and 3nd-party systems). Certificates are independent and isolated from each other.		
27		The SDN controller should support the ability to integrate with OSS management systems, and super controllers by providing a unified North interface, without the need for multiple components to provide multiple north-interface		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
28		The SDN controller should support BGP-LS in compliance with following RFCs: - RFC 7752 - North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP - RFC 3784 - ISIS TE support - RFC 5305 - IS-IS Extensions for Traffic Engineering - RFC 4271 - A Border Gateway Protocol 4 (BGP-4) - RFC 6793 - BGP Support for Four-Octet Autonomous System (AS) Number Space - RFC 4360 - BGP Extended Communities Attribute - RFC 1997 - BGP Communities Attribute - RFC 5575 - Dissemination of Flow Specification Rules - RFC 4724 - Graceful Restart Mechanism for BGP - draft-gredler-idr-bgp-ls-segment-routing-ext - BGP Link-State extensions for Segment Routing - draft-ietf-idr-flowspec-redirect-ip-02.txt - BGP Flow-Spec Redirect to IP Action - draft-ietf-idr-wide-bgp-communities-01 - Wide BGP Communities Attribute - draft-ietf-idr-flowspec-interfaceset-03 - Applying BGP flowspec rules on a specific interface set - draft-gredler-idr-bgp-ls-segment-routing-ext-02 - BGP Link-State extensions for Segment Routing		
29		Controllers can prevent unauthorized disclosure of sensitive data. Unauthorized entities and individuals cannot obtain the data because of the following protection policies:		
30		The Network Management System (NMS) shall be carrier-grade and highly scalable. It must support a license capacity of at least 20,000 Network Elements (NEs) within a single management domain or cluster, ensuring the system can handle the complete NEA network expansion for the next 7 years without platform replacement.		
31		SDN service control and management interfaces are unified, providing consistent O&M experience. The NMS should integrate the Manager and Controller, unify the data layer, software deployment, HA		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
		solution, UI style, and O&M, and provide an end-to-end solution.		
32		Bandwidth adjustment: NMS should improve the utilization of network resources and support L1/L2 services and service adjustment (e.g., ODU/Flex/CAR/MPLS-TP) where applicable to the overall transport solution.		
33		The NMS must support intelligent event management, alarm compression, and root cause analysis.		
34		The NMS must support topology view management, including searching for, expanding, and collapsing topology views, viewing NE connection information and topology object attributes, and editing topology objects.		
35		The NMS must support the NTP server configuration of NEs and the NMS, and support the configuration and management of NE time and time zone.		
36		The NMS supports fault management, alarm browsing, and alarm setting.		
37		The NMS must support performance management, performance information browsing, and performance setting.		
38		The NMS must support inventory management, statistics on physical inventory of NEs, fiber and fiber management, adding, modifying, and deleting a single fiber or fiber/cable, and SDH/WDM inventory report management.		
39		The NMS must support NMS security management, including user, role, region, object, operation set, and online user management. Supports NMS access control management, forcible user logout, access control list setting, user access time and IP address range, and changing the user name and password of the NMS, operating system, and database.		
40		The NMS must support log management, query and export of operation logs, system logs, and security logs of base station controllers, and support user-defined conditions for automatic log dumping. NE operation logs and security logs can be queried and		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
		exported.		
41		The NMS must support NE software management, NE configuration management, NE backup and restoration, and NE upgrade and downgrade. Supports manual and periodic NE backup.		
42		NMS supports online software upgrades without affecting services.		
43		NMS must support data migration from traditional network management systems to NMS.		
44		The NMS must support remote disaster recovery deployment, minute-level failover, and arbitration-free nodes.		
45		The SDN controller must support IP traffic adjustment based on IPFIX/sFlow and BGP Flow Specification.		
46		The SDN controller should support outbound service flow adjustment based on destination IP address		
47		The SDN controller should support outbound service flow adjustment based on destination AS		
48	Cross-Layer Synergy & SRLG Synchronization	To prevent network blackouts, the NMS must support Cross-Domain Synergy between the IP and Optical layers. The Optical system shall automatically share Shared Risk Link Group (SRLG) data with the IP Routers. This ensures that the Router's IGP/MPLS control plane does not inadvertently route both the Primary and Backup paths over the same physical fiber duct. The solution shall demonstrate One-Click provisioning where an IP link creation automatically triggers the necessary Optical path setup.		

1.3 DWDM network Solution technical Specifications.

The capabilities of the offered equipment should comply with the detailed technical specifications (including DWDM devices, Core routers, DC PE Routers, Aggregation Routers, Core IGW Router, NMS for backbone network) in the condition of the additional required components (e.g. accessories, service boards, license, etc.).

1.3.1 DWDM Devices

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
1	Network Design	a) Consider the OSNR tolerated by the transponder, based on Recommendation G.698.2		
2		b) Consider the minimum defined OSNR based on Recommendation G.698.2		
3		c) Consider the maximum OSNR penalty for the optical route defined in Recommendation G.698.2, plus an additional fiber margin of 3dB. This calculation must also be considered for the EOL conditions.		
4		d) Consider in the project design of the solution, the penalty resulting from the chromatic dispersion, calculated for the optical path considered;		
5		e) Consider in the project design of the solution, the penalty derived from the slope of the chromatic dispersion, calculated for the optical path considered;		
6		f) Consider in the design of the solution project the penalty resulting from the dispersion due to the polarization mode (PMD), calculated for the optical path considered;		
7		g) Consider in the project design of the solution, the penalty resulting from non-linear effects, optical crosstalk effects, attenuation due to optical filters, cascade effect on optical filter width, polarization dependent losses, amplifiers, Mux / demux, dispersion compensator modules, add / drop modules, etc.		
8		h) Consider in the design of the solution design, the maximum value and minimum value of the average input power, in the transponders defined in Recommendation G.698.2		
9	Standards and Recommendations	The proposed equipment must comply with the latest revisions of the Standards cited in this item		
10		Environmental conditions - Standard ETSI - ETS 300 019-2-3 – Environmental Conditions and environmental tests for telecommunication equipment. Part 2-3: Specification of		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
		environmental tests - Stationary use at weather protected Locations;		
11		Ventilation and thermal performance of racks and sub-racks - ETSI standard - EN 300 119-5 - European telecommunication standard for equipment practice; Part 5 -Thermal management;		
12		Direct current supply - ETSI - Environment engineering (EE) standard; Power supply interface at the input to telecommunications equipment; Part 2: Operated by direct current (dc).		
13		Optical Safety: IEC 60825-1; IEC 60825-2;		
14		IEC 60825.1 Safety of Laser Product, Part 1: equipment classification, Requirements and user's guide		
15		IEC 60825.2: 2004 + A1: 2006 Safety of Laser Product, Part 2: Safety of optical fiber Communications systems (OFCS);		
16		The Electromagnetic Interference(EMI), Susceptibility(EMS) of equipment should comply with EN 55032, IEC/EN 61000-6-2, IEC/EN 61000-6-4, IEEE 1613, IEC 61850-3, the bidder should provide the related test report.		
17		The bidding equipment should acquire the CC certificate issued by FIPS/NSCIB/BSI or the equivalent organization.		
18		The bidding equipment must have participated in recognized international interoperability testing events (such as EANTC, JITC, or IETF Plugfests) within the last three years, demonstrating successful interoperability and feature maturity.		
19	Practices and Recommendations for DWDM Equipment	G.652 Characteristics of a single-mode optical fiber and cable		
20		G.653 Characteristics of a dispersion-shifted single-mode optical fiber and cable		
21		G.655 Characteristics of a non-zero dispersion-shifted single-mode optical fiber		
22		G.661 Definitions and test methods for the relevant generic parameters of optical Amplifier devices and subsystems		
23		G.662 Generic characteristics of optical amplifier devices and subsystems		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
24		G.663 Application related aspects of optical amplifier devices and subsystems		
25		G.664 Optical safety procedures and requirements for optical transport system		
26		G. 665 Generic characteristics of Raman amplifiers and Raman amplified		
27		G.671 Transmission characteristics of optical components and subsystems		
28		G.691 Optical interfaces for single channel STM-64 and other SDH systems with Optical Amplifiers		
29		G. 692 Optical interfaces for multichannel systems with optical amplifiers		
30		G.693 Optical interfaces for intra-office systems		
31		G.694.1 Spectral Grids for WDM Applications: DWDM Frequency Grid;		
32		G.696.1 Intra sound compatible DWDM applications longitudinally		
33		G.697 Optical monitoring for DWDM systems		
34		G.698.2 Single channel optical channel amplified multichannel DWDM applications Interfaces		
35		G.703 - Physical / electrical characteristics of hierarchical digital interfaces		
36		G.707 - Network node interface for the synchronous digital hierarchy (SDH);		
37		G.709 / Y.1331 Interfaces for the Optical Transport Network (OTN)		
38		G.783 - Features of Synchronous Digital Hierarchy (SDH) Functional blocks;		
39		G.798 - Characteristics of the optical transport network hierarchy Functional Blocks		
40		G.803 - Transport-network architecture based on the digital synchronous system Hierarchy (SDH)		
41		G.805 Generic functional architecture of transport networks		
42		G.806 Characteristics of transport equipment - Methodology of description and Generic functionalities		
43		G.808.1 Generic protection switching - Linear and subnetting protection;		
44		G.825 - The control of fluctuation and drift in digital networks which are based In the synchronous digital hierarchy (SDH)		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
45		G.841 - Types and characteristics of SDH network protection architectures		
46		G.870 / Y.1352 Terms and definitions for Optical Transport Networks (OTN)		
47		G.871 / Y.1301 Framework for the optical transport network Recommendations		
48		G.872 The functional architecture of optical transport networks using modelling Methodology described in G. 805;		
49		G.873.1 Optical Transport Network (OTN): Linear Protection		
50		G.874 Management aspects of optical transport network elements		
51		G.957 Optical interfaces for equipment and systems relating to the synchronous Digital hierarchy		
52		G.959.1 Optical transport network physical layer interfaces		
53		G.7041 / Y.1303 Generic framing procedure (GFP)		
54		G.7042 / Y.1305 Link capacity adjustment scheme (LCAS) for virtual concatenated		
55		G.7710 / Y.1701 Common equipment management function requirements		
56		G.8201 Error performance parameters and objectives for multi-operator International paths within the Optical Transport Network (OTN);		
57		M.3010 Principles for a telecommunications management network		
58		IEEE 802.3 part 3: Carrier sense multiple access with collision detection (CSMA / CD) access method and physical layer specification		
59	System Architecture for OTN Equipment	The bidding electrical-layer equipment should support the OTN architecture, separate tributary boards and line boards, and have centralized and unified PKT/VC/ODUk switching boards to facilitate smooth service upgrade and evolution.		
60		The offered system should be ROADM architecture with Directionless & Flex grid for each site, in order to support 400G/800G/1.2T/1.6T per wavelength.		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
61	Optical Path	An optical path or optical path or light path is defined as the route made by a signal Optical (wavelength) WDM, without undergoing optical-electric-optical conversion, since Line from the source transponder to the line destiny. In this trajectory the optical signal passes through optical elements that can include Optical multiplex / demultiplex with channel inserts / drift, optical amplifiers, Optical dispersion compensator modules, optical connectors, etc.		
62	Fiber Parameters	All fibers are of type G652. Consideration should be given to the standard. Reference of Rec G.652 for Chromatic Dispersion (ps / nm.km) and Slope S0 (ps / nm2 Km) At 1550nm.		
63	Network Performance	The network must operate in a manner that ensures reliability, availability and quality in service delivery, with performance such that it guarantees a Bit Error Rate equal to or greater than 10^{-12} guaranteed in the client interfaces of each channel in operation		
64	Network Optical Transients	Optical amplifiers, which make up the network, must have characteristics that allow fast and automatic control of these transients.		
65		The monitoring and adjustment points must provide dynamic and fully automatic equalization of the optical signal in order to maintain the specified performance for the network without degradation of the quality of service.		
66	Monitoring, Alarms, Settings	The proposed solution should provide alarm monitoring and OTS optical transmission section, multiplex (OMS optical multiplex section) and optical channel (OCh) end to end, as per the latest revisions of ITU-T Recommendations G.709, G.697 and other Recommendations and Norms		
67		The proposed solution should detect anomalies and defects and take action in accordance with ITU-T Recommendation G.783.		
68		The proposed solution should implement automatic signal degradation monitoring, fault monitoring, and channel tuning. This monitoring must be done in each carrier through an optical spectrum analyzer integrated with the equipment and through the processing of the information		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
		carried by the OSC channel		
69		The proposed solution must implement adjustment and equalization of the power of each channel, continuously and automatically, acting on transponders and / or optical amplifiers and / or multiplex / demultiplex with channel insertion / drift capability.		
70		The adjustment action must occur completely automatically. No optical power adjustment action, in this context, should require operator intervention to be performed.		
71		The proposed solution should have monitoring points to allow measurements to be made through optical analyzers or other external measurement equipment without the impact of traffic on the line signal.		
72		The proposed solution should implement monitoring of at least the following parameters, making this information available through the proposed management system. Total optical power in the line; Optical power per channel; OSNR on each channel;		
73	Supervision Channel – OSC	The proposed equipment shall implement an Optical Supervisory Channel (OSC) with functionalities, characteristics and performance in accordance with the latest revisions of the Recommendations.		
74		The OSC channel must be processed and supervised at all stations in the network.		
75		In the case of a station with multiple directions (degrees), the OSC channel must be available and processed in each of the existing directions.		
76		The OSC channel shall provide a data communication channel which, in addition to other functions, shall carry the optical route control information.		
77		The OSC channel must reach the receiver of the adjacent station with sufficient OSNR to be correctly processed.		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
78	DWDM functionality with OTN	The cross-connect capability of the bidding equipment is greater than or equal to 4.8 Tbps ODUk, not less than 4.8 Tbps Packet.The system can groom OTN services, SDH services, and packet services on the same device, simplifying the networking mode in which SDH devices are connected to OTN devices to groom SDH services.		
79		The DWDM system shall operate in the Extended C-Band with a minimum usable optical spectrum width of 4.8 THz. To ensure future-proofing, the system shall be design-capable of supporting a minimum of 96 channels at 50GHz spacing. The solution must support seamless evolution to increase total fiber capacity to at least 192 channels (via L-Band addition or C-Band spectrum expansion) without interrupting existing services.		
80		The bidding equipment should support 120 lambda with 50GHz channel space in C band frequency with 100G, 200G (120ch*100G@50GHz and 120ch*200G@50GHz) end-to-end transmission capabilities, including service boards, optical and demultiplexer boards, OA boards, and optical monitoring boards.		
81		The bidding equipment shall support WSS/ROADM architectures for wavelength grooming with reference the topology for fixed grid(75 GHz/50 GHz) wavelength signal and flexible grid(n x slice GHz (n=6~64, 1 slice=6.25GHz)) wavelength signal operation.		
82		The 100G/200G/400G/600G/800G line interfaces should support the tuning of the carrier frequency optical module on all the working channels defined in ITU-T Recommendation G.694.1		
83		The bidding equipment should have the ability to flexible converge FE/GE/STM-1/STM-4/STM-16/STM-64/10GE LAN&WAN and 1GFC/2GFC/4GFC/8GFC/12GFC/16GFC/32GFC /ESCON/25GE/40GE/50GE/100GE/400GE to 10G/100G/200G/400G/600G/800G wavelengths directly without cascading transponders/muxponders or OTN equipments.		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
84	Protection switching requirements	The bidding equipment should use the OTN architecture and support ODUk_SNCP (subnet connection) protection. The switching time must be less than 50 ms.		
85		The bidding equipment shall support the LAG/DLAG/MC-LAG protection for L2 Ethernet features		
86		The bidding equipment shall support the ERPS/PW APS/Tunnel APS protection for L2 Ethernet features		
87		The bidding equipment should support the implementation of GMPLS (RFC 3945) and ASON (ITU-T G.8080)		
88		The bidding equipment must support optical-layer/electrical-layer ASON, and can provide application cases for the bidding OTN products of the same type successfully enabling the ASON function and operating for at least one year.		
89		The bidding equipment supports the AES256 encryption function at the L1 layer. The encryption function must be configured at the channel level to meet the security requirements of different services within the same wavelength. The product documentation must be provided for proof.		
90		The power supply, control, clock, and cross-connect boards of the bidding equipment must be configured with 1+1 protection. For boards with hot backup, the active and standby boards can be forcibly switched over through the NMS, and the NMS screenshots must be provided for proof.		
91		OTN client side protection should be supported		
92	OTN GMPLS requirements	The system must comply with the ASON/GMPLS standard recommended by the ITU-T and IETF.		
93		The equipment must support the I-NNI, and complies with the signalling, routing, and link management protocols.		
94		The link management protocol should allow users to enable and disable TE link check.		
95		Users should be allowed to modify TE link names.		
96		Route computation should consider the customized cost of TE links.		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
97		Link management should support a shared risk link group (SRLG).		
98		The control plane should support automatic discovery of the network topology and network resources.		
99		ASON/GMPLS should support the calculation of the source node route.		
100		The routing algorithm should support the constraint-based route computation.		
101		The routing algorithm should support the route computation based on traffic balancing.		
102		ASON/GMPLS supports the path pre-calculation function for an end-to-end service.		
103		ASON/GMPLS should allow users to enable or disable the OSPF protocol.		
104	Requirements of Network Protection and restoration	In order to cope with simultaneous multiple failures both protection and restoration functionalities shall be provided. Protection functionality shall be provided for all types of traffic, normal and high priority (for both present and final service requirements) traffics. Restoration functionality shall be provided on the top of protection functionality for all high priority traffic (for both present and final service requirements).		
105		Protection switch of **normal** (present and final) priority traffic shall be triggered on optical power monitoring and there shall be provision to set the LOS thresholds.		
106		Automatic switching, user-initiated manual and forced switching, as well as lockout shall be supported.		
107		Automatic switching for the high priority traffic demands shall be triggered by line faults (LOS, LOF,…), or ODU layer faults.		
108		Sequential restoration in case of multiple failure is desirable for high priority traffic.		
109		If, after clearing of fault the main or the protection path becomes available, then the restored traffic shall return to the original path automatically.		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
110		Bidder shall provide detail protection and restoration plans separately for the normal and high priority traffic and for both the present and final service requirements. Such a plan is given in Annex 1.4 for understanding of the bidder.		
111	Optical Amplifiers	The amplifiers must have fully automatic mechanisms that allow the control of gain and / or power and optimize the spectral flatness of their gain.		
112		Their operational characteristics shall comply with the specifications for response to the optical transients of the network specified.		
113		The chromatic dispersion and dispersion compensators due to polarization mode (PMD), when used in the solution, shall be in accordance with the latest revisions to the Recommendations referred in this Technical Specification and others relevant to the subject.		
114	Operation and Maintenance	The optical power, OSNR, and wavelength values of all wavelengths must be monitored. Performance parameters such as 10G/100G/200G/400G/600G/800G OSNR can be reported to the NMS and E2E 10G/100G/200G/400G/600G/800G OSNR can be managed online. The detection precision must reach +/-1.5 dB. The corresponding product manual is provided.		
115		The DWDM system shall support Integrated Online OTDR functionality to monitor fiber quality (attenuation, events) without interrupting services. The OTDR capabilities shall be controlled via the NMS, allowing for automated periodic scanning and on-demand troubleshooting from the control center.		
116		The functionality is capable of indicating the distance, in meters and / or kilometers, between a station and the point of discontinuity of the fiber, with an accuracy of at least 3m, when the optical fibers that form the link between two stations , Provided that such break has occurred within a distance of up to 150 km from one of the link stations.		

Item	Subject matter	Technical Specification	Comply (Yes/No)	Remarks
117		A single management system must be provided for all DWDM / OTN equipment offered.		
118		The bidding equipment should supports latency detection using the NMS. The NMS screenshots of the latency detection must be provided, and the corresponding product documentation must be provided.		
119	Environmental conditions	To ensure heat dissipation and maintenance, the electrical-layer subrack must have multiple independent fan trays to facilitate maintenance and system stability.		
120		The bidding equipment must support 1+1 63 A or 2+2 63 A power input to reduce the power supply requirements for the equipment room.		
121		Comply to ETSI Class 3.1 stnrdard, the temperature range: Storage (ETS 300 019-1-1): –40°C～+70°C Transport (ETS 300 019-1-2): –40°C～+70°C Operation (ETS 300 019-1-3): Long-term operating temperature: 0°C to 45°C, Short-term operating temperature: -5°C to 50°C		
122		The bidding equipment must support DC power supply modes. DC power input range Standard operating voltage: -48 V to -60 V Operating voltage range: -40 V to -72 V		

1.3.2 Core Routers

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
1	Route & MPLS Feature	Support RIP, OSPF, IS-IS, BGP,BGP4+, RIPng, OSPFv3, IS-ISv6.		
2		Support static routes, multicast static routes		
3		Support IPv4/IPv6 Dual Stack.		
4		Support routing policy.		
5		Support load balancing in unequal cost multiple path mode.		
6		Support MD5 and keychain authentication for IGP and BGP.		
7		Support MPLS LDP and MPLS RSVP-TE.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
8		Support LDP and TE FRR, support configure the FRR switching within 200ms.		
9		Support SR-BE, SR-TE and SR Policy.		
10		Support SRv6 BE and SRv6 TE Policy.		
11		Support EVPN VPWS & EVPN VPLS & EVPN L3VPN over SRv6 TE policy		
12		Support SR-MPLS TI-LFA/Anti-micro-loop.		
13		Support SRv6 TI-LFA, Anti-micro-loop, mirror sid.		
14		Support VPLS/VPWS and L3VPN.		
15		Support EVPN VPLS/VPWS/L3VPN.		
16		Support Bier/Bierv6.		
17		Support SRv6 Service Function Chain (SFC).		
18	L2 Features	Support VLAN and VxLAN services.		
19		Support bridge domain and EVC Layer 2 sub-interface.		
20		Support Eth-Trunk interfaces and BFD for eth-trunk to detect the eth-trunk interface status.		
21	QoS scalability	Support 5-Level Hierarchical QoS.		
22		Support PQ, WFQ and LPQ.		
23	High Availability Feature	Support hardware BFD. BFD detect package send period should within 3.3ms.		
24		Support BFD for VRRP, OSPF, ISIS, BGP, LDP, TE, SR, VRRPv6, OSPFv3, ISISv6, BGP4+,PW.		
25		Support Remote-LFA/TI-LFA/Anti-micro-loop.		
26		Support VRRP.		
27		Support Ethernet in the First Mile and connectivity Fault Management.		
28		Support In-band real-time service monitoring, fast failure location and visualization on the SDN controller.		
29		Support SRv6 TE FRR & SRv6 TI-LFA & BFD for SRv6 TE Policy.		
30	Synchronization	Support frequency synchronization via synchronous ethernet (SyncE) on all Ethernet interfaces.		
31		Support time synchronization via 1588v2 and G.8275.1 profile on all Ethernet interfaces.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
32	Certificates	The proposed routers should have certificate of MEF 3.0 Carrier Ethernet.		
33		The proposed router must be offered by an OEM that has been recognized in the Gartner Magic Quadrant for Service Provider Routers (or equivalent relevant Gartner report) as a Leader or a Challenger for at least two of the last three publication years.		
34		The proposed routers must have participated in recognized international interoperability testing events (such as EANTC, JITC, or IETF Plugfests) within the last three years, demonstrating successful interoperability and feature maturity.		
35		The proposed routers should have certificate of CC EAL4+ or FIPS 140-2 Level 2 or equivalent third-party security certification.		
36	Key Features	Support a forwarding plane architecture that enables future feature expansion via software upgrade, with minimal to no hardware replacement cost.		
37		Provide 28*100GE+10*10GE/GE ports and 40G@1024bytes IPsec throughput,500 IPsec tunnels in day one.		
38		Support system capacity larger than 6.4 Tbps (full duplex) for day one.		
39		Support no less than 64*100GE for the device model.		
40		Support non-blocking switching fabric to allow wire speed forwarding on all interfaces and line card.		
41		Support control plane completely independent of the forwarding plane		
42		Support at least 8 services slots for flexible expansion in the future.		
43		Support 800G per slot in switching fabric redundancy mode for day one.		
44		Support 400GE/100GE/40GE/10GE/GE interface.		
45		Support 1:1 redundancy for the control plane.		
46		Support redundancy for AC power supplies and fans.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
47		Support IPv4/v6 RIB not less than 60M/30M.		
48		Support IPv4/v6 FIB not less than 6M/3M.		
49		Support VLL instances not less than 64K.		
50		Support VPLS VSI instances not less than 32K.		
51		Support IPv4/v6 VRF instance not less than 16K/16K.		

1.3.3 DC PE Routers

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
1	Route & MPLS Feature	Support RIP, OSPF, IS-IS, BGP,BGP4+, RIPng, OSPFv3, IS-ISv6.		
2		Support static routes, multicast static routes		
3		Support IPv4/IPv6 Dual Stack.		
4		Support routing policy.		
5		Support load balancing in unequal cost multiple path mode.		
6		Support MD5 and keychain authentication for IGP and BGP.		
7		Support MPLS LDP and MPLS RSVP-TE.		
8		Support LDP and TE FRR, support configure the FRR switching within 200ms.		
9		Support SR-BE, SR-TE and SR Policy.		
10		Support SRv6 BE and SRv6 TE Policy.		
11		Support EVPN VPWS & EVPN VPLS & EVPN L3VPN over SRv6 TE policy		
12		Support SR-MPLS TI-LFA/Anti-micro-loop.		
13		Support SRv6 TI-LFA, Anti-micro-loop, mirror sid.		
14		Support VPLS/VPWS and L3VPN.		
15		Support EVPN VPLS/VPWS/L3VPN.		
16		Support Bier/Bierv6.		
17		Support SRv6 Service Function Chain (SFC).		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
18	L2 Features	Support VLAN and VxLAN services.		
19		Support bridge domain and EVC Layer 2 sub-interface.		
20		Support Eth-Trunk interfaces and BFD for eth-trunk to detect the eth-trunk interface status.		
21	QoS scalability	Support 5-Level Hierarchical QoS.		
22		Support PQ, WFQ and LPQ.		
23	High Availability Feature	Support hardware BFD. BFD detect package send period should within 3.3ms.		
24		Support BFD for VRRP, OSPF, ISIS, BGP, LDP, TE, SR, VRRPv6, OSPFv3, ISISv6, BGP4+,PW.		
25		Support Remote-LFA/TI-LFA/Anti-micro-loop.		
26		Support VRRP.		
27		Support Ethernet in the First Mile and connectivity Fault Management.		
28		Support standard In-band Flow Telemetry mechanisms (such as IETF standard In-situ OAM or equivalent) to provide real-time service quality monitoring (latency, jitter, packet loss) at the service flow level. This capability must be supported on the Access node to ensure end-to-end fault demarcation from the remote substation to the control center.		
29		Support SRv6 TE FRR & SRv6 TI-LFA & BFD for SRv6 TE Policy.		
30	Synchronization	Support frequency synchronization via synchronous ethernet (SyncE) on all Ethernet interfaces.		
31		Support time synchronization via 1588v2 and G.8275.1 profile on all Ethernet interfaces.		
32	Certificates	The proposed routers should have certificate of MEF 3.0 Carrier Ethernet.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
33		The proposed routers should be among the top 3 global market share (including enterprise and service provider) in 2022, 2023 and 2024 in terms of revenue based on IDC report.		
34		The proposed routers must have participated in recognized international interoperability testing events (such as EANTC, JITC, or IETF Plugfests) within the last three years, demonstrating successful interoperability and feature maturity.		
35		The proposed routers should have certificate of CC EAL4+.		
36	Key Features	Support a forwarding plane architecture that enables future feature expansion via software upgrade, with minimal to no hardware replacement cost.		
37		Provide 8*100GE+16*10GE/GE in day one.		
38		Support system capacity larger than 2.4Tbps (full duplex) for the day one.		
39		Support no less than 24*100GE for the device model.		
40		Support at least 6 services slots for flexible expansion in the future.		
41		Support 400GE/100GE/40GE/10GE/GE interface.		
42		Support 1:1 redundancy for the control plane and forwarding plane.		
43		Support redundancy for AC power supplies and fans.		
44		Support IPv4/v6 RIB not less than 28M/10M.		
45		Support IPv4/v6 FIB not less than 6M/3M.		
46		Support VLL instances not less than 64K.		
47		Support VPLS VSI instances not less than 16K.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
48		Support IPv4/v6 VRF instance not less than 16K/16K.		

1.3.4 AGG Routers

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
1	Route & MPLS Feature	Support RIP, OSPF, IS-IS, BGP,BGP4+, RIPng, OSPFv3, IS-ISv6.		
2		Support static routes, multicast static routes		
3		Support IPv4/IPv6 Dual Stack.		
4		Support routing policy.		
5		Support load balancing in unequal cost multiple path mode.		
6		Support MD5 and keychain authentication for IGP and BGP.		
7		Support MPLS LDP and MPLS RSVP-TE.		
8		Support LDP and TE FRR, support configure the FRR switching within 200ms.		
9		Support SR-BE, SR-TE and SR Policy.		
10		Support SRv6 BE and SRv6 TE Policy.		
11		Support EVPN VPWS & EVPN VPLS & EVPN L3VPN over SRv6 TE policy		
12		Support SR-MPLS TI-LFA/Anti-micro-loop.		
13		Support SRv6 TI-LFA, Anti-micro-loop, mirror sid.		
14		Support VPLS/VPWS and L3VPN.		
15		Support EVPN VPLS/VPWS/L3VPN.		
16		Support Bier/Bierv6.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
17		Support SRv6 Service Function Chain (SFC).		
18	L2 Features	Support VLAN and VxLAN services.		
19		Support bridge domain and EVC Layer 2 sub-interface.		
20		Support Eth-Trunk interfaces and BFD for eth-trunk to detect the eth-trunk interface status.		
21	QoS scalability	Support 5-Level Hierarchical QoS.		
22		Support PQ, WFQ and LPQ.		
23	High Availability Feature	Support hardware BFD. BFD detect package send period should within 3.3ms.		
24		Support BFD for VRRP, OSPF, ISIS, BGP, LDP, TE, SR, VRRPv6, OSPFv3, ISISv6, BGP4+,PW.		
25		Support Remote-LFA/TI-LFA/Anti-micro-loop.		
26		Support VRRP.		
27		Support Ethernet in the First Mile and connectivity Fault Management.		
28		Support standard In-band Flow Telemetry mechanisms (such as IETF standard In-situ OAM or equivalent) to provide real-time service quality monitoring (latency, jitter, packet loss) at the service flow level. This capability must be supported on the Access node to ensure end-to-end fault demarcation from the remote substation to the control center.		
29		Support SRv6 TE FRR & SRv6 TI-LFA & BFD for SRv6 TE Policy.		
30	Synchronization	Support frequency synchronization via synchronous ethernet (SyncE) on all Ethernet interfaces.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
31		Support time synchronization via 1588v2 and G.8275.1 profile on all Ethernet interfaces.		
32	Certificates	The proposed routers should have certificate of MEF 3.0 Carrier Ethernet.		
33		The proposed routers should be among the top 3 global market share (including enterprise and service provider) in 2022, 2023 and 2024 in terms of revenue based on IDC report.		
34		The proposed equipment series must have participated in recognized international interoperability testing events (such as EANTC, JITC, or IETF Plugfests) within the last three years, demonstrating successful interoperability and feature maturity.		
35		The proposed routers should have certificate of CC EAL4+.		
36	Key Features	Support a forwarding plane architecture that enables future feature expansion via software upgrade, with minimal to no hardware replacement cost.		
37		Provide 2*100GE+2*10GE/GE ports and 200M@1024bytes IPsec throughput,100 IPsec tunnels in day one.		
38		Support system capacity larger than 1.2Tbps (full duplex) for the day one.		
39		Support no less than 12*100GE/80*10GE for the device model.		
40		Support maximum system capacity larger than 2.4Tbps (full duplex) for		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
		the device model.		
41		Support at least 4 services slots for flexible expansion in the future.		
42		Support 400GE/100GE/40GE/10GE/GE interface.		
43		Support 1:1 redundancy for the control plane and forwarding plane.		
44		Support redundancy for AC power supplies and fans.		
45		Support IPv4/v6 RIB not less than 10M/5M.		
46		Support IPv4/v6 FIB not less than 4M/2M.		
47		Support VLL instances not less than 64K.		
48		Support VPLS VSI instances not less than 16K.		
49		Support IPv4/v6 VRF instance not less than 16K/16K.		

1.3.5 Access Routers

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
1	Route & MPLS Feature	Support RIP, OSPF, IS-IS, BGP,BGP4+, RIPng, OSPFv3, IS-ISv6.		
2		Support static routes, multicast static routes		
3		Support IPv4/IPv6 Dual Stack.		
4		Support routing policy.		
5		Support load balancing in unequal cost multiple path mode.		
6		Support MD5 and keychain authentication for IGP and BGP.		
7		Support MPLS LDP and MPLS RSVP-TE.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
8		Support LDP and TE FRR, support configure the FRR switching within 200ms.		
9		Support SR-BE, SR-TE and SR Policy.		
10		Support SRv6 BE and SRv6 TE Policy.		
11		Support EVPN VPWS & EVPN VPLS & EVPN L3VPN over SRv6 TE policy		
12		Support SR-MPLS TI-LFA/Anti-micro-loop.		
13		Support SRv6 TI-LFA, Anti-micro-loop, mirror sid.		
14		Support VPLS/VPWS and L3VPN.		
15		Support EVPN VPLS/VPWS/L3VPN.		
16		Support Bier/Bierv6.		
17		Support SRv6 Service Function Chain (SFC).		
18	L2 Features	Support VLAN and VxLAN services.		
19		Support bridge domain and EVC Layer 2 sub-interface.		
20		Support Eth-Trunk interfaces and BFD for eth-trunk to detect the eth-trunk interface status.		
21	QoS scalability	Support 5-Level Hierarchical QoS.		
22		Support PQ, WFQ and LPQ.		
23	High Availability Feature	Support hardware BFD. BFD detect package send period should within 3.3ms.		
24		Support BFD for VRRP, OSPF, ISIS, BGP, LDP, TE, SR, VRRPv6, OSPFv3, ISISv6, BGP4+,PW.		
25		Support Remote-LFA/TI-LFA/Anti-micro-loop.		
26		Support VRRP.		
27		Support Ethernet in the First Mile and connectivity Fault Management.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
28		Support standard In-band Flow Telemetry mechanisms (such as IETF standard In-situ OAM or equivalent) to provide real-time service quality monitoring (latency, jitter, packet loss) at the service flow level. This capability must be supported on the Access node to ensure end-to-end fault demarcation from the remote substation to the control center.		
29		Support SRv6 TE FRR & SRv6 TI-LFA & BFD for SRv6 TE Policy.		
30	Synchronization	Support frequency synchronization via synchronous ethernet (SyncE) on all Ethernet interfaces.		
31		Support time synchronization via 1588v2 and G.8275.1 profile on all Ethernet interfaces.		
32	Certificates	The proposed routers should have certificate of MEF 3.0 Carrier Ethernet.		
33		The proposed routers should be among the top 3 global market share (including enterprise and service provider) in 2022, 2023 and 2024 in terms of revenue based on IDC report.		
34		The proposed equipment series must have participated in recognized international interoperability testing events (such as EANTC, JITC, or IETF Plugfests) within the last three years, demonstrating successful interoperability and feature maturity.		
35		The proposed routers should have certificate of CC EAL4+.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
36	Key Features	Support a forwarding plane architecture that enables future feature expansion via software upgrade, with minimal to no hardware replacement cost.		
37		Provide 4*10GE+12*GE ports and 200M@1024bytes IPsec throughput,100 IPsec tunnels in day one.		
38		Support system capacity larger than 160 Gbps (full duplex) for the day one.		
39		Support no less than 16*10GE for the device model.		
40		Support 10GE/GE interface.		
41		Support redundancy for AC power supplies and fans.		
42		Support IPv4/v6 RIB not less than 512K/256K.		
43		Support IPv4/v6 FIB not less than 512K/256K.		
44		Support VLL instances not less than 8K.		
45		Support VPLS VSI instances not less than 4K.		
46		Support IPv4/v6 VRF instance not less than 2K.		

1.3.6 CORE IGW Routers

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
1	Route & MPLS Feature	Support RIP, OSPF, IS-IS, BGP,BGP4+, RIPng, OSPFv3, IS-ISv6.		
2		Support static routes, multicast static routes		
3		Support IPv4/IPv6 Dual Stack.		
4		Support routing policy.		
5		Support load balancing in unequal cost multiple path mode.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
6		Support MD5 and keychain authentication for IGP and BGP.		
7		Support MPLS LDP and MPLS RSVP-TE.		
8		Support LDP and TE FRR, support configure the FRR switching within 200ms.		
9		Support SR-BE, SR-TE and SR Policy.		
10		Support SRv6 BE and SRv6 TE Policy.		
11		Support EVPN VPWS & EVPN VPLS & EVPN L3VPN over SRv6 TE policy		
12		Support SR-MPLS TI-LFA/Anti-micro-loop.		
13		Support SRv6 TI-LFA, Anti-micro-loop, mirror sid.		
14		Support VPLS/VPWS and L3VPN.		
15		Support EVPN VPLS/VPWS/L3VPN.		
16		Support Bier/Bierv6.		
17		Support SRv6 Service Function Chain (SFC).		
18	L2 Features	Support VLAN and VxLAN services.		
19		Support bridge domain and EVC Layer 2 sub-interface.		
20		Support Eth-Trunk interfaces and BFD for eth-trunk to detect the eth-trunk interface status.		
21	QoS scalability	Support 5-Level Hierarchical QoS.		
22		Support PQ, WFQ and LPQ.		
23	High Availability Feature	Support hardware BFD. BFD detect package send period should within 3.3ms.		
24		Support BFD for VRRP, OSPF, ISIS, BGP, LDP, TE, SR, VRRPv6, OSPFv3, ISISv6, BGP4+,PW.		
25		Support Remote-LFA/TI-LFA/Anti-micro-loop.		
26		Support VRRP.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
27		Support Ethernet in the First Mile and connectivity Fault Management.		
28		Support standard In-band Flow Telemetry mechanisms (such as IETF standard In-situ OAM or equivalent) to provide real-time service quality monitoring (latency, jitter, packet loss) at the service flow level. This capability must be supported on the Access node to ensure end-to-end fault demarcation from the remote substation to the control center.		
29		Support SRv6 TE FRR & SRv6 TI-LFA & BFD for SRv6 TE Policy.		
30	Synchronization	Support frequency synchronization via synchronous ethernet (SyncE) on all Ethernet interfaces.		
31		Support time synchronization via 1588v2 and G.8275.1 profile on all Ethernet interfaces.		
32	Certificates	The proposed routers should have certificate of MEF 3.0 Carrier Ethernet.		
33		The proposed routers should be among the top 3 global market share (including enterprise and service provider) in 2022, 2023 and 2024 in terms of revenue based on IDC report.		
34		The proposed equipment series must have participated in recognized international interoperability testing events (such as EANTC, JITC, or IETF Plugfests) within the last three years, demonstrating successful interoperability and feature maturity.		
35		The proposed routers should have certificate of CC EAL4+.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
36	Key Features	Support a forwarding plane architecture that enables future feature expansion via software upgrade, with minimal to no hardware replacement cost.		
37		Provide 6*100GE+10*10GE/GE in day one.		
38		Support system capacity no less than 1.2Tbps (full duplex) for the day one.		
39		Support no less than 8*100GE and 48*10GE for the device model.		
40		Support 100GE/40GE/10GE/GE interface.		
41		Support redundancy for AC power supplies and fans.		
42		Support IPv4/v6 RIB not less than 25M/10M.		
43		Support IPv4/v6 FIB not less than 4M/2M.		
44		Support VLL instances not less than 16K.		
45		Support VPLS VSI instances not less than 10K.		
46		Support IPv4/v6 VRF instance not less than 16K/16K.		

1.3.7 Network management System of National Backbone Network

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
1	Management System	The network management system is unique for any solution offered		
2		The Management System and its respective hardware have a management capacity of at least 5 (five) times the number of elements of the proposed network, as informed in this Technical Specification.		
3		The Network Management System to be deployed will also manage any of the network elements that are provided.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
4		The Management System allows the backup of all the configuration information of the network elements, so as to guarantee the maintenance of the operability of both the network and the management system, in any failure situation.		
5		The Management System makes it possible to download the configurations of the network elements, to perform their update in cases of failure and also to update the software of these elements in cases of system upgrade.		
6		The Management System has a maximum of two (2) distinct levels of management. One level of network management and another level of element management.		
7		All the configuration of the equipment is made through the management system, which should even allow the software update remotely, through specific commands.		
8		Access to each network element through the management system is protected by passwords in security level categories.		
9	SPECIFIC TECHNICAL REQUIREMENTS OF THE MANAGEMENT SYSTEM	NMS complies with the mainstream SDN architecture defined by Internet Engineering Task Force (IETF). This architecture consists of a device layer, a controller layer, an orchestration layer, and an application layer.		
10		NMS is capable of full-service lifecycle management, capability exposure, and intensive, automated, and intelligent operation and maintenance (O&M).		
11		NMS provides unified user interfaces (UIs) for network management, control, and analysis.		
12		NMS can manage legacy devices. It manages and controls legacy networks and SDN networks in the same way.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
13		NMS provides a unified portal. All functions are available on this portal, and users do not need to open different systems.		
14		NMS complies with mainstream IETF and Abstraction and Control of Traffic Engineered Networks (ACTN) standards.		
15		NMS supports Representational State Transfer (REST) interfaces and Yet Another Next Generation (YANG) models.		
16		NMS complies with the following YANG language standards: RFC 6991, RFC 7951, RFC 7950, and RFC 7895.		
17		Data transmission channels support secure protocols, such as Hypertext Transfer Protocol Secure (HTTPS), Simple Network Management Protocol Version 3 (SNMPv3), and Transport Layer Security (TLS).		
18		Web application firewall (WAFs) can be deployed to defend against SQL injection, cross-site scripting attacks, malicious code protection, and application-layer denial of service attacks.		
19		Data is transmitted on networks at the risk of being eavesdropped, tampered, or copied and resent. Controllers need to implement end-to-end (E2E) encryption on various interfaces.		
20		SSL/TLS protocol: supports the TLSv1.2 protocol released by IETF.		
21		Internal channels: use HTTPS to encrypt the data exchanged among management services (such as the installation, monitoring, upgrade, and maintenance services).		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
22		Support Account policy: - Minimum number of characters in the account name - Max. number of inactive days - Lockout upon consecutive login failures - IP address range - Account lockout policy - Login time range - Max. consecutive failed login attempts - Account lockout duration (if not permanent) - Auto delete long locked or disabled accounts - Log out of unauthorized sessions		
23		Support Password policy: - At least three types of characters (uppercase letters, lowercase letters, digits, and special characters) - Min. password length - Previous passwords disallowed - Max. times a character can occur - Min. interval between password change operations - Min. special characters - Enforce password expiration - Password validity period - Days of warnings prior to password expiration - Log out of the current session after password reset - Weak password dictionary		
24		Controllers can record complete logs about its own status, security events, operations, and configurations for query and audit, real-time check, analysis, and protection.		
25		System logs record abnormal status and actions when NMS is running, such as failure to execute scheduled tasks.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
26		The NMS uses different CA certificates for different peer systems (northbound, southbound, and 3nd-party systems). Certificates are independent and isolated from each other.		
27		The SDN controller should support the ability to integrate with OSS management systems, and super controllers by providing a unified North interface, without the need for multiple components to provide multiple north-interface		
28		The SDN controller should support BGP-LS in compliance with following RFCs: -RFC 7752 - North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP -RFC 3784 - ISIS TE support -RFC 5305 - IS-IS Extensions for Traffic Engineering -RFC 4271 - A Border Gateway Protocol 4 (BGP-4) -RFC 6793 - BGP Support for Four-Octet Autonomous System (AS) Number Space -RFC 4360 - BGP Extended Communities Attribute -RFC 1997 - BGP Communities Attribute -RFC 5575 - Dissemination of Flow Specification Rules -RFC 4724 - Graceful Restart Mechanism for BGP - draft-gredler-idr-bgp-ls-segment-routing-ext - BGP Link-State extensions for Segment Routing - draft-ietf-idr-flowspec-redirect-ip-02.txt - BGP Flow-Spec Redirect to IP Action - draft-ietf-idr-wide-bgp-communities-01 - Wide BGP Communities Attribute		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
		- drft-ietf-idr-flowspec-interfaceset-03 - Applying BGP flowspec rules on a specific interface set - draft-gredler-idr-bgp-ls-segment-routing-ext-02 - BGP Link-State extensions for Segment Routing		
29		Controllers can prevent unauthorized disclosure of sensitive data. Unauthorized entities and individuals cannot obtain the data because of the following protection policies:		
30		The entire network is managed as a whole. Large networks (30,000 ENEs) could be managed.		
31		SDN service control and management interfaces are unified, providing consistent O&M experience. The Network Management System (NMS) shall provide a Unified Single-Pane-of-Glass view for both the Optical (OTN/DWDM) and IP (Router) layers. It must support end-to-end service provisioning (L0 to L3) and cross-layer fault correlation from a single graphical user interface (GUI) without the need for the operator to launch separate applications or switch context. The solution must demonstrate One-Click service creation across layers.		
32		Bandwidth adjustment :NMS should improve the utilization of network resources. Layer 1 services support the ODU flex technology, and Layer 2 services support the CAR+ ODU flex bandwidth adjustment technology.		
33		The NMS must support intelligent event management, alarm compression, and root cause analysis.		
34		The NMS must support topology view management, including searching for,		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
		expanding, and collapsing topology views, viewing NE connection information and topology object attributes, and editing topology objects.		
35		The NMS must support the NTP server configuration of NEs and the NMS, and support the configuration and management of NE time and time zone.		
36		The NMS supports fault management, alarm browsing, and alarm setting.		
37		The NMS must support performance management, performance information browsing, and performance setting.		
38		The NMS must support inventory management, statistics on physical inventory of NEs, fiber and fiber management, adding, modifying, and deleting a single fiber or fiber/cable, and SDH/WDM inventory report management.		
39		The NMS must support NMS security management, including user, role, region, object, operation set, and online user management. Supports NMS access control management, forcible user logout, access control list setting, user access time and IP address range, and changing the user name and password of the NMS, operating system, and database.		
40		The NMS must support log management, query and export of operation logs, system logs, and security logs of base station controllers, and support user-defined conditions for automatic log dumping. NE operation logs and security logs can be queried and exported.		
41		The NMS must support NE software management, NE configuration management,		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
		NE backup and restoration, and NE upgrade and downgrade. Supports manual and periodic NE backup.		
42		NMS supports online software upgrades without affecting services.		
43		NMS must support data migration from traditional network management systems to NMS.		
44		The NMS must support remote disaster recovery deployment, minute-level failover, and arbitration-free nodes.		
45		The SDN controller must support IP traffic adjustment based on netsteam/Bgp-flowspec.		
46		The SDN controller should support outbound service flow adjustment based on destination IP address		
47		The SDN controller should support outbound service flow adjustment based on destination AS		

1.3.8 Power Supply Devices

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
1	Ambient Temperature	Operating temperature range: –10°C to +45°C. Storage and transportation temperature range: –40°C to +70°C.		
2	Ambient Humidity	Operating relative humidity: 5% to 95% (non-condensing) Relative humidity for storage and transportation: 5% to 95% (non-condensing)		
3	Altitude	Altitude: 0–4000 m. When the altitude ranges from 2000 m to 4000 m, the operating temperature is derated by 1°C for each additional 200 m.		
4	Vibration Performance	The power system should be able to withstand the sine wave vibration with the frequency of 10–55 Hz and amplitude of 0.35 mm.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
5	Maintenance	1) All operations and O&M must be performed from the front or rear of the cabinet. The monitoring module, rectifiers, circuit breakers, fuses, and other modules must be placed at the front of the cabinet to facilitate maintenance. 2) The product must provide sufficient space for operation and maintenance. The circuit breakers and buttons for operation must be flexible and reliable. To facilitate maintenance, cables should be routed from the top of the cabinet. 3) Both the monitoring module and the rectifier module are hot-swappable. Replacing the monitoring module does not affect the normal running of the system.		
6	System Capacity	Normal Sites: 1) The maximum capacity of the system is not less than 24 kW, the number of power module slots is not less than 6, and the power density is not less than 7 kW/U 2) The power system capacity expansion should be supported. Region Sites: 1) The maximum capacity > 60 KW 2) power modules slot is not less than 18		
7	AC input	The system supports AC power supply. One 3-pole circuit breaker(no less than 63 A) should be configured for AC input. AC input mode: 220/380 V three-phase, four-wire, compatible with 220 V single-phase Allowed voltage range: 85–300 V AC, rated voltage range: 220–240 V AC. The output power is linearly derated between 175–85 V AC, and full rate between 176–300 V AC Allowed frequency range: 45 Hz to 66 Hz. When the rated input voltage and full output load are used, the total harmonic distortion (THD) of the input current should be less than or equal to 5%.		
8	Rectifier	Rectifiers should support grid input 3 phase balancing to ensure that no single phase overcurrent causes power failure.		
9		Normal Sites: the rectifier should support solar input, PSU slot should be interoperable with Solar supply unit.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
10	DC output protection	Normal Sites: The system should provide DC output protection as below 1) DC output overvoltage and undervoltage protection 2) DC output overcurrent and short circuit protection 3) Load low voltage disconnection (LLVD) 4) Battery low voltage protection (BLVD) Region Sites: remove LLVD, other same as above		
11	Size	Normal Sites DC Distribution Unit 1) The height of the DC power distribution circuit breaker cannot exceed 1 U. 2) The DC power distribution circuit breaker is hot-swappable, facilitating maintenance. Change to number of breakers for DC output		
12	System voltage drop	The internal voltage drop (between the battery input port and load output port) does not exceed 500 mV (full load test at 20°C).		
13	Inter-module current sharing	1) The rectifiers in the system can work in parallel mode. The current of each module can be automatically balanced to achieve current equalization. If the system is loaded with 20% to 100% loads, the imbalance between rectifiers is less than or equal to ±5%. If a rectifier is faulty, the system can still work properly. 2) When the monitoring unit is faulty, the rectifiers should be able to automatically balance the current (and describe how the system controls the current).		
14	Surge protection	Normal Sites: 1) The AC input end of the system should be configured with level B surge protection (standard lightning discharge current: 30 kA, 8/20 μs). The system should provide the anti-reverse connection function. 2) The DC output end should be equipped with a surge protective device (SPD) to withstand impulse current (10 kA in differential mode and 20 kA in common mode). Region Sites: 1) The AC input end of the system should be configured with level B surge protection (standard lightning discharge current: 20/40 kA, 8/20 μs). The system should provide the anti-reverse connection function.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
		2) The DC output end should be equipped with a surge protective device (SPD) to withstand impulse current (10/20 kA).		
15	Electrostatic discharge (ESD) immunity	The system should be able to protect against electrostatic damage and the protection should comply with criterion B of EN 61000-4-2 level 3. The system should also be able to withstand 8 kV air discharge and 6 kV contact discharge.		
16	Noise voltage	The peak-to-peak noise voltage of the system DC output end in the 0 MHz to 20 MHz frequency band should be less than or equal to 200 mV.		
17	System Reliability	a) MTBF: not less than 3 x 105 hours at 30°C (excluding batteries) b) The system should last for 10 years by design.		
18	Monitoring Module	The monitoring module provides the following functions: 1) With LCD display function (LCD screen); 2) Monitors the system operating status in real time, including but not limited to the operating status of the entire system, rectifiers, battery strings, and power distribution units. 3) Collects and stores system running parameters, including but not limited to the full parameters of Power system, Rectifier module, Rectifier group, Battery string 4) Sets the parameters of the system and modules including but are not limited to System control mode, LLVD power-on and power-off voltage, AC overvoltage and undervoltage alarm thresholds, DC overvoltage and undervoltage alarm thresholds, alarm management of the power system; Default output voltage, minimum number of working rectifiers of the rectifiers; Rated capacity, equalized and float charge voltage, BLVD power-on and power-off		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
		voltage, BLVD time and capacity, high temperature protection mode and voltage, high/low temperature alarm threshold of the battery, etc. 5) Clears alarms automatically after errors are cleared. 6) Provides RS232 and RS485 communications ports. 7) Supports communication over an Ethernet port and complies with SNMPv3. 8) Supports IP, GPRS, and in-band networking. 9) Supports hot swap for easy replacement and maintenance.		
19	Rectifier	1) When the rated voltage and load rate are 30%–80%, the rectifier efficiency should be greater than or equal to 95%. 2) The maximum efficiency of rectifiers can reach 97%. 3) A rectifier does not exceed 1 U in height and 2.5 U in width. 4) Maximum rated power of rectifiers: Not less than 4000 W 5) High-temperature power derating feature: The rectifiers work in full load at a temperature lower than 55°C. The bidder should provide the temperature and power output curve. 6) The input power factor of the rectifiers should be not less than 0.99 at 100% load, not less than 0.98 at 50% load, not less than0.97 at 20% load 7) Rectifiers should be highly reliable. The MTBF should be greater than or equal to 500,000 hours.		
20	Battery	Battery should Valve Regulated Lead Acid Battery Type of battery must be AGM/GEL Battery case should be fireproof with certain certification or rating Height of the battery should not be more than 8U		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
21	Qualification	The products of the equipment provider should be reviewed and tested annually by qualified intermediary assessment agencies and testing centers. The equipment provider should have the following certificates: 1) ISO 9001 series quality management system certificate 2) OHSAS 18000 occupational health and safety management system certificate 3) ISO 14000 environmental management system certificate 4) The equipment provider should have the following qualifications: a) The telecom power system is used by more than 50 carriers worldwide and a user list should be provided. b) The telecom power system has been applied to more than 10 tier-1 carriers and an acceptance report should be provided. c) The telecom power products have been put into commercial use for more than three years, and the acceptance certificate should be provided.		
22	Output Capacity	DC output Capacity of each offered rectifier module is 75 A (4000W)		
23	Redundancy	Rectifier modules redundancy should be N+1		
24	Cabling mode	Top Cabling		
25	Battery Brunch	DC Distribution Normal Sites: Battery Branch: 3 x 125 MCB LLVD Branch: 2 x 125A MCB, 4 x 63A MCB, 4 x 32A MCB BLVD Branch: 8 x 32A MCB, 1 x 16A MCB Region Sites: Battery Branch: 2 x 1000 A Load Branch: 4 x 500A（NT3），2x400A（NT2），6x160A（NT00），6x100A（NT00）		
26	Power System Installation type	Standard 19” rack		

1.3.9 Site Power Supply Equipment Management System

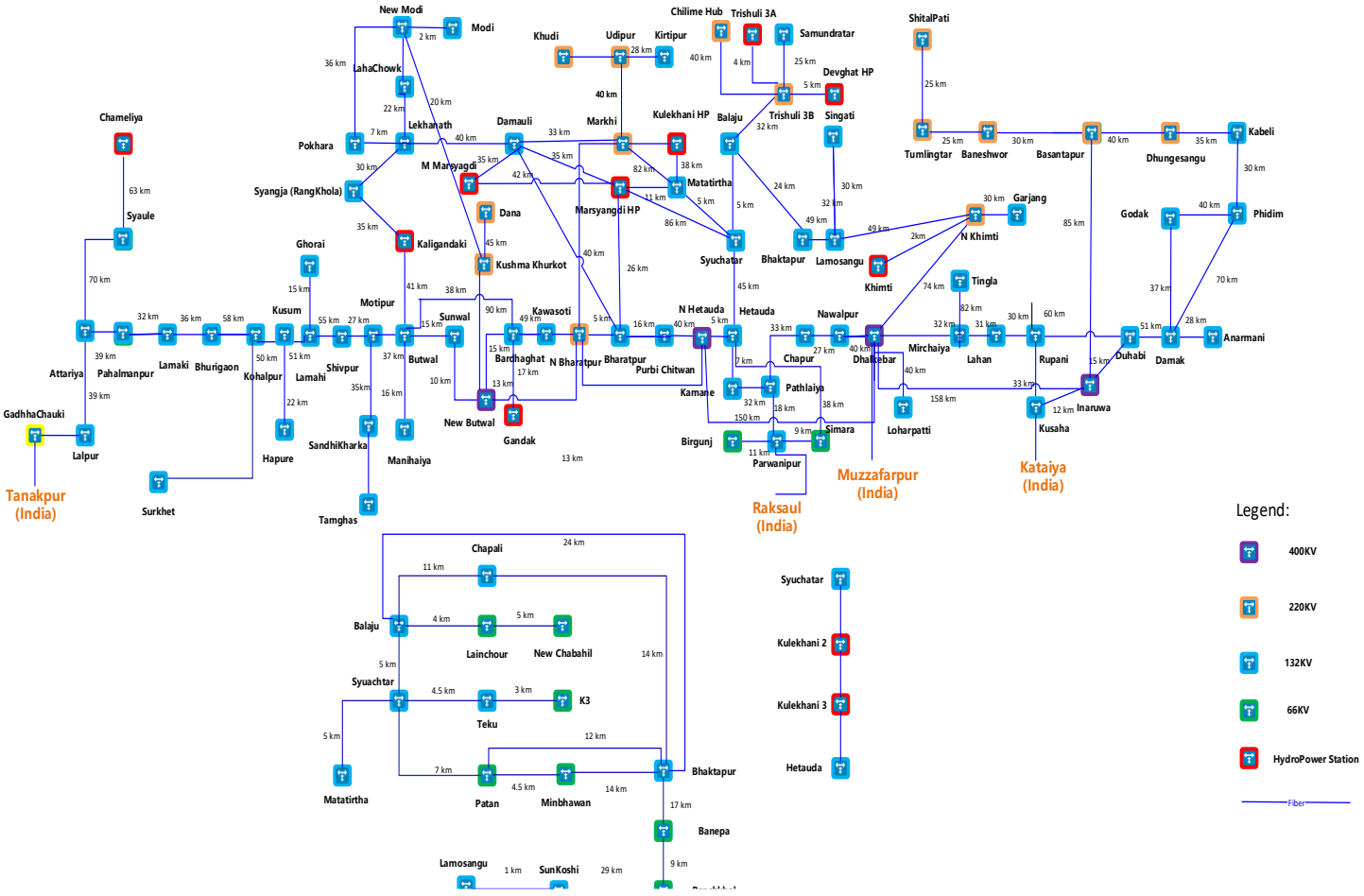
Item	Subject matter	Specification	Comply (Yes/No)	Remarks
1	System Architecture	The management system should use the browser/server (B/S) structure. Users can log into the system using a browser without installing management software. The client/server (C/S) structure is unacceptable.		
2		The management system should provide northbound interface (NBI) to report alarms and performance data to the upper-layer management system for unified management.		
3	Management Capability	The management platform should be able to manage at least 2000 sites, and max.10,000 sites.		
4		The NMS should support the standard protocol like SNMP/FTP/Webservices		
5	Site Networking	The NMS should support multiple networking modes, such as IP, 2G, 3G, 4G,etc. To implement site access management in different scenarios.		
6	Alarm Management	The NMS should support alarm browsing : Current alarm browsing, historical alarm browsing, masked alarm browsing, real-time alarm reminder, alarm analysis.		
7		The NMS should support alarm processing: Alarm acknowledgement and un-acknowledgement, Alarm clearance, Alarm handling guidance and expert maintenance experience library, Alarm log synchronization.		
8		The NMS should support alarm setting: Masking rules, Correlation rules, Identification rules, Intermittent/Toggling rules, Aggregation relation rules, Alarm sounds, Dry contact alarm management, Alarm redefinition, Automatic alarm dump, Alarm threshold .		
9		The NMS should support Remote alarm notification.		
10	Monitoring Features	The NMS should support GIS site navigation.		
11		The NMS should support network-level real-time monitoring.		
12		The NMS should support site information overview.		
13		The NMS should support graphical user interface and energy flow.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
14	Configuration Management	The NMS should support rapid site deployment: Automatic discovery of sites, Visualized and quick site deployment, Batch site deployment and site planning, Remote commissioning and acceptance.		
15		The NMS should support configuration data management :Configuration data synchronization, Parameter modification in batches, Configuration data export, Signal management.		
16	Performance and Report	The NMS should support performance data collection and storage, Performance data query, Root Cause Analysis for Site Shutdown.		
17		NMS will support site energy efficiency analysis and data report.		
18		NMS should support power availability analysis and data report.		
19		NMS should support carbon emission dashboard and data report.		
20		The NMS should support root cause analysis for site shutdown		
21		The NMS should support report Management :Favourite report management, Power Availability Analysis Report, Energy efficiency and consumption report, Bit/watt synergy report, Power supply proportion report, Mains energy consumption comparison report, Temperature control running report, Mains running report (including power outage and mains quality analysis).		
22		The NMS should support battery running report, Energy supply equipment run log, Site environment report, Site disconnection (the communication between NMS server and NE).		
23		The NMS should support statistic report, SIM card usage statistic report, Load running report, Real-time inventory report, Customized report, Report task management).		
24	System and User Security	The NMS should support system security management.		
25		The NMS should support user right management.		
26		The NMS should support access security management (Security policy, Online user management, User access list, Mobile App user management).		
27		The NMS should support NE user management.		

Item	Subject matter	Specification	Comply (Yes/No)	Remarks
28	Rectifier software lock	The proposed system shall support advanced asset security features to prevent unauthorized removal of modules. The system shall include mechanisms (such as electronic locking, software pairing, or anti-theft alarms) that trigger an alert in the NMS if a rectifier module is removed without authorization		

NEA backbone:

Below is the existing OPGW backbone network of NEA.



2. Technical Specifications: SCADA (refer Volume-II, Part-B)

Please refer to Volume-II, Part-B for the detailed and complete SCADA technical specifications.

Volume-II, Part-B includes the scope and requirements of the SCADA solutions. This covers the introductory overview of SCADA, its core functions and integration, user interface requirements, system software and hardware specifications, configuration guidelines, and system availability criteria.

Volume-II, Part-B also provides detailed requirements related to testing and documentation, including technical specifications for Hardware and software requirements of SCADA solutions., Remote Terminal Units (RTUs), MFTs, transducers, and communication modems, along with the necessary test equipment for RTU validation.

Volume-II, Part-B further includes specifications and clearly defines the scope of support services, such as AMS, ATS and FMS and associated Service Level Agreements (SLAs) to ensure ongoing operational reliability. Furthermore, it presents the design parameters and detailed Bills of Quantities (BOQs) for all software and hardware components of SCADA required for implementation at both the Distribution Control Center (DCC) and the Backup Control Center (BCC/DRC).

3. Technical Specifications: ADSS (refer Volume-II, Part-C)

Please refer to Volume-II, Part-C for the detailed ADSS technical specifications.

The illustrative survey provided below is tentative. The System Integrator (SI) shall be responsible for conducting a final detailed site survey. The actual optical fiber requirement shall be determined based on this survey and duly approved by the NEA

While estimated cable route lengths are included for reference, the Contractor shall supply and install ADSS Optical Fiber Cable as per the final site conditions identified during project execution.

----- End of Chapter 3 -----

CHAPTER 4: SERVICE LEVEL AGREEMENTS (SLA)

Implementation stage SLA:

SLA Parameter	Condition	Penalty
Delay in implementation milestone	<= 1 week	No Penalty
Delay in implementation milestone	>1 week to < 4 Weeks	0.5% of the milestone payment
Delay in implementation milestone	>= 4 to < 6 Weeks	1% of the milestone payment
Delay in implementation milestone	>= 6 to < 8 Weeks	1.5% of the milestone payment
Delay in implementation milestone	> 8 Weeks	Additional 1% for every week's delay beyond 8th week capped at 10% of total project capex
Delays in milestones attributable to SI	2 Occasions	No Penalty
If the Key Personnels are not available without intimation or timely replacement (Yearly Measurement - Penalty will be applied in second year's payments)	Per Occasion	NPR 50,000/- per person

* Note: -

Only one replacement of per profile would be permitted per year. Replacement due to reasons not in control of SI (like resignation of the resource, accident, etc.) would not be counted in the permissible replacement.

SLA Network Infrastructure related SLA

Sl. No.	Service	Parameter	Requirement	Service Level	Measurement Tool /Validation	Penalty (on Quarterly Payment)
1	DWDM, OTN, Fiber & NOC	Overall Network Availability of NOC & Core PoPs	>=99.95 % uptime	All the Network Equipment installed and commissioned	**≥99.99**	No Penalty
					≥99.5 % to <99.99%	1%
					≥99.0% to <99.5%	3%
					99%	Additional 1% penalty on account of each 0.1%

						reduction in uptime (maximum 10% of project cost)

Network Availability (%) for a month = (Total minutes during the month – Downtime minutes during the month) *100 / Total minutes during the month.

Network Equipment Availability for a month = Total time (in minutes) in a month - total down time (in minutes) in a month The network is considered available when all the services in full capacity are available.

Total Time shall be measured on 24*7 basis. The downtime of the Aggregation, Pre- Aggregation, Spur PoPs and Access locations commissioned during the implementation phase shall be calculated on pro-rata basis.

Measurement Tool: Reports from NOC duly approved by NEA Project Manager. SI shall submit quarterly reports on the performance and adherence to the SLA The SLA for end office locations shall be measured from the time of the call being registered.

SLA SCADA System and RTU Availability

Please refer to **CHAPTER 14, Part-B OF Volume-II, for** the Service SLA related to SCADA solutions, as detailed in the SCADA technical specifications section.

---- End of Chapter 4 -----

CHAPTER 5: TESTS (FAT & UAT)

Factory Acceptance Tests

Factory acceptance tests shall be conducted on randomly selected final assemblies of all equipment to be supplied. Factory acceptance testing shall be carried out on OTN/DWDM/Router/NMS Equipments.

Equipment shall not be shipped to the Employer until required factory tests are completed satisfactorily, all variances are resolved, full test documentation has been delivered to the Employer, and the Employer has issued Material Inspection & Clearance Certificate (MICC). Successful completion of the factory tests and the Employer approval to ship. These tests shall be carried out in the presence of the Employer's authorized representatives unless waiver for witnessing by Employer's representatives is intimated to the contractor.

Factory acceptance tests shall not proceed without the prior delivery and approval of all test documentation by the Employer.

The factory acceptance test shall demonstrate the technical characteristics of the equipment in relation to these specifications and approved drawings and documents. List of factory acceptance tests for OTN/DWDM/Router system and NMS are given in specified Tables in this section. This list of factory acceptance tests shall be supplemented by the Contractor's standard FAT testing program. The factory acceptance tests for the other items shall be proposed by the Contractor in accordance with technical specifications and Contractor's (including Sub-Contractor's / suppliers) standard FAT testing program. In general the FAT for other items shall include at least: Physical verification, demonstration of technical characteristics, various operational modes, functional interfaces, alarms and diagnostics etc. For Test equipment & clock, FAT shall include supply of proper calibration certificates, demonstration of satisfactory performance, evidence of correct equipment configuration and manufacturer's final inspection certificate/ report.

Cybersecurity Vulnerability Scan: During FAT, the equipment must undergo a vulnerability scan using industry-standard tools (e.g., Nessus, Qualys) to demonstrate hardening against known CVEs. The vendor must provide a 'Security Hardening Guide' specific to the proposed version.

1.1 Sampling for FAT (Network Solutions)

Since FAT testing provides a measure of assurance that the Quality Control objectives are being met during all phases of production, the Employer reserves the right to require the Contractor to investigate and report on the cause of FAT failures and to suspend further testing/ approvals until such a report is made and remedial actions taken, as applicable.

Table 1: Factory Acceptance Testing for OTN/DWDM/Router/NMS System

FAT on OTN	
1	GE Service Access Test
2	E1 Service Access Test
3	2M Optic Service Access Test
4	64K Sub-rate Service Access Test
5	Legacy Service Functionality Test: Verification of Hotline or direct-connection voice circuits between substations using the proposed PCM solution (Internal or External).
6	Service card transmit optical power
7	Service card receiver Sensitivity
8	E1 SNCP Protection function Test
9	Packet SNCP Protection function
10	System control Board Protection Test
11	Power Supply Card Protection Test

FAT on DWDM	
1	100GE Service Test
2	Service card transmit optical power
3	Service card receiver Sensitivity
4	Optical Amplifier Gain Test
5	ODUk SNCP function Test
6	System control Board Protect Test
7	Power Supply Card Protect Test
8	Equipment Built-in OTDR function Test

FAT on Router	
1	System Power-on
2	Logging in through HyperTerminal
3	MPU slave switch
4	Power 1+1 backup
5	Voltage Monitoring

FAT on NMS	
1	Topology management Test
2	Alarm Management Test
3	Service Management Test

1.2 Testing of SCADA Solutions

Please refer to Chapter-7 of Volume-II, Part-B for the detailed and complete testing and documentation of SCADA System.

1.3 Testing of RTU's

Please refer to Chapter-11 of Volume-II, Part-B for the detailed and complete testing and documentation of RTU's.

----- End of Chapter 5 -----

CHAPTER 6: BILL OF MATERIAL

This chapter outlines the comprehensive Bill of Material (BoM) essential for the project covering all major materials including ADSS fiber optic cabling, Optical Transport Network (OTN) systems, Dense Wavelength Division Multiplexing (DWDM) solutions, and SCADA-related components. Each section provides detailed quantities and specifications of materials and equipment required for implementation, installation, and commissioning, ensuring alignment with technical standards and operational needs. This BoM serves as a critical reference for procurement planning, execution, and quality assurance across all work packages. However, the final BOM will be considered as mentioned in the Volume III of this RFP.

1. Bill of Material (ADSS)

Part -C	Fiber	UOM	QTY
1	48F ADSS fiber optic cable	Kms	8000
2	Termination/Tension Assembly including anchor/D-Shackle, Thimble, Turn Buckle, Extension Rods, Protective Helix, Termination Helix and any or all other associated accessories and fittings	Nos	16000
3	Suspension Assembly including twisted link, clevis thimble, suspension helix, protective helix and any or all other associated accessories and fittings	Nos	40000
4	Pole Stay Clamps with all fittings (with vibration dampers-as per standard)	Nos	20964
5	Adjustable Cable Storage Brackets with all associated accessories and fittings	Nos	6988
6	Fiber Optic Splice Enclosure (Joint Box-IP68/Waterproof) for ADSS with associated pole mounting accessories	Nos	1300
7	Spiral Vibration Damper	Nos	2000
8	Fiber Distribution Management System (FDMS), 48F with all accessories	Nos	504
09	Cable Tray	Mtr	2000
10	Simplex Plug	Nos	464

2. Bill of Material (OTN Solution)

Part -D	OT network (OTN)	UOM	QTY
A	**OTN Device**		
1	**OTN Equipment (OTU4)** with 2 degree OTU4 (1 working port + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	110

2	**OTN Equipment (OTU4)** with 3 degree OTU4 (2 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	57
3	**OTN Equipment (OTU4)** with 4 degree OTU4 (3 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	15
4	**OTN Equipment (OTU4)** with 5 degree OTU4 (4 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	4
5	**OTN Equipment (OTU4)** with 6 degree OTU2 (5 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	20
6	**OTN Equipment (OTU4)** with 7 degree OTU2 (6 working ports + 1 spare port), supporting 10G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	4
7	**OTN Equipment (OTU4)** with 8 degree OTU2 (7 working ports + 1 spare port), supporting 10G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	4
8	**OTN Equipment (OTU2)** with 9 degree OTU4 (8 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	2
9	**OTN Equipment (OTU4)** with 10 degree OTU4 (9 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	2
10	**OTN Equipment (OTU4)** with 11 degree OTU4 (9 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	1
11	**OTN Equipment (OTU4)** with 12 degree OTU4 (9 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	1

12	**OTN Equipment (OTU4)** with 14 degree OTU4 (13 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	1
13	**OTN Equipment (OTU4)** with 16 degree OTU4 (15 working ports + 1 spare port), supporting 100G line, 10*GE, 32*E1, DDN, FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	1
14	**OTN Equipment (OTU4) for Syuachtar** with 7 degree OTU4 (6 working ports + 1 spare port), supporting 100G line, 20*GE, 210*E1, DDN, 210*FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	1
15	**OTN Equipment (OTU4) for New Butwal** with 3 degree OTU4 (2 working ports + 1 spare port), supporting 100G line, 20*GE, 210*E1, DDN, 210*FXS/FXO, 8*2M Optical service access, including software license and installation material	Set	1
16	24U (1200x600x800 mm) Rack for OTN (including Rack frame with front/rear doors, 2x PDUs (15A), 1x Fan tray, Grounding kit, Cable manager, Mounting rails)	Nos	224
B	**Site Power Device**		
1	110 V DC to 48 V DC converter with all accessories, cable etc for backup power to Router, OUT and DWDM devices.	Nos	272

3. Bill of Material (DWDM Solution)

Part -F	IT Network-DWDM Solution	UOM	QTY
Part -E	**IT Network**		
A	**DWDM**		
1	**DWDM Device,** Extended C-Band (Min 4.8THz usable width) OR Super C-band system, 2-Degree OLA sites, including Installation Material and license	Set	15
2	**DWDM Device,** Extended C-Band (Min 4.8THz usable width) OR Super C-band system, 3-Degree OLA sites, including Installation Material and license	Set	1
3	**DWDM Device,** Extended C-Band (Min 4.8THz usable width) OR Super C-band system, 4-Degree OLA sites, including Installation Material and license	Set	1
4	**DWDM Device,** Extended C-Band (Min 4.8THz usable width) OR Super C-band system, 9-Degree ROADM with directionless & flexgrid architecture, 2*100GE access (with 2*100G QSFP28 0.1km),	Set	12

	line side use 2*200G (200G/λ, with 2*200G CFP), including optical amplifier, Installation Material and license		
5	**DWDM Device, New Butwal** Extended C-Band (Min 4.8THz usable width) OR Super C-band system, 9-Degree ROADM with directionless & flexgrid architecture, 16*100GE (with 16*100G QSFP28 0.1km) access, line side use 12*200G (200G/λ, with 12*200G CFP) and 1*400G(200G/λ, with 1*400G CFP), including optical amplifier, Installation Material and license	Set	1
6	**DWDM Device, Syuachtar** Extended C-Band (Min 4.8THz usable width) OR Super C-band system, 9-Degree ROADM with directionless & flexgrid architecture, 16*100GE (with 16*100G QSFP28 0.1km) access, line side use 12*200G (200G/λ, with 12*200G CFP) and 1*400G(200G/λ, with 1*400G CFP), including optical amplifier, Installation Material and license	Set	1
7	**Core Router Device,** Redundancy on control-boards and AC power modules, with 28*100GE(16*QSFP28 0.1km, 4*QSFP28 10km, 4*QSFP28 40km), 10*10GE/GE(5*SFP+ 10km; 5*SFP 10km), 40G IPsec throughput & 500 IPsec tunnel and software license for necessary	Nos	2
8	**IGW Router Device,** Redundancy on control-boards and AC power modules, with 6*100GE(3*QSFP28 0.1km, 1*QSFP28 40km), 10*10GE/GE(5*SFP+ 10km; 5*SFP 10km), and software license for necessary	Nos	4
9	**DC PE Router Device,** Redundancy on control-boards and AC power modules, with 8*100GE(4*QSFP28 0.1km)+16*10GE/GE(8*SFP+ 10km; 8*SFP 10km) and software license for necessary	Nos	4
10	**AGG Router Device,** Redundancy on control-boards and AC power modules, with 2*100GE(2*QSFP28 0.1km), 10*10GE/GE(5*SFP+ 10km; 5*SFP 10km), 200M IPsec throughput & 100 IPsec tunnel and software license for necessary	Nos	14
11	**ACC Router Device,** Redundancy on AC power modules, with 4*10GE(2*SFP+ 80km, 2*SFP+ 10km) , 12*GE(at least 4 electric GE ports, 8*SFP 10km), 200M IPsec throughput & 100 IPsec tunnel and software license for necessary	Nos	129
B	**Site Power Device**		
1	110 V DC to 48 V DC converter with all accessories, cable etc for backup power to Router, OUT and DWDM devices.	Nos	184

4. Bill of Material (SCADA Solution, LDMS & RTU)

Please refer to Table-8 BOQ (Bill of Material: SCADA) -Volume-II, Part-B for the detailed and complete SCADA technical specifications.

----- End of Chapter 6 -----

Appendix

LIST OF ABBREVIATIONS

- ADSS: All-Dielectric Self-Supporting
- ANSI: American National Standards Institute
- AMC: Annual Maintenance Contract
- AOR: Area of Responsibility
- BCC: Backup Control Center
- BOQ: Bill of quantity
- CB: Circuit Breaker
- CMR: Contact Multiplying Relay
- CIM: Common Information Model
- CMOT: Common Management Information Protocol
- COSEM: Companion Specification for Energy Metering
- CPU: Central Processing Unit
- CRM:- Customer Relationship Management
- CSMA/CD :- Carrier Sense Multiple Access With Collision Detection
- DCC: Distribution command center/SCADA Control center
- DAT: Digital Audio Tap
- DC: Data Concentrator
- DCPS: DC Power Supply System
- DDoS: Distributed Denial of Service
- DLMS: Device Language message specification
- DMZ: Demilitarized zone
- DNS:- Domain Name System
- DR: Data Recovery
- DRC: Disaster Recovery Center
- DRR: Disaster Replica Recovery
- DSF :- Dispersion-shifted fiber
- DTS: Dispatcher training simulator
- DWDM- Dense Wavelength Division Multiplexer
- EDFAs :- Erbium-doped fiber amplifiers
- EWS – Engineering Work Station
- FAT: Factory Acceptance Test
- FE/GE :- Fast Ethernet / Gigabit Ethernet

- FEC: Forward Error Correction
- FODP:-Fibre Optic Distribution Panels
- FODB:- Fibre Optic Distribution Box
- FMS: Facility Management Services
- FTP: File Transfer Protocol
- ESB: Enterprise service bus
- ECMA: European Computer Manufacturers Association
- FCC: Federal Communications Commission
- FRS:- Functional Requirement Specification
- GOOSE: Generic Object-Oriented Substation Even
- GPS: Global positioning system
- GPRS: General Packet Radio Service
- GUI : Graphical User Interface
- HDR: Heavy Duty Relays
- HDD: Hard Disk Drive
- HI : Historian Information
- HIPS: Host-based IPS
- HTTP : Hyper Text Transfer Protocol
- HT- High Tension
- H/W - Hardware
- ICCCM: Inter-Client Communications Conventions Manual
- ICCP: Inter Control Center Protocol
- ICS: Industrial Control System
- IEC: International Electro technical commission
- IEEE: - Institute of Electrical and Electronics Engineers
- IGW: Internet Gateway
- IOT :- Internet of Things
- IPS: Intrusion prevention system
- ISP: Internet Service Provider
- ISO: International organizations for standardizations
- IEC: International Electrotechnical Commission
- IEEE: - Institute of Electrical and Electronics Engineer
- ISR: Information storage & retrievals
- IRIG: Inter-Range Instrumentation Group
- IT : Information Technology

- LAN: Local Area Network
- LDAP: Lightweight Directory Access Protocol
- LDMS Local Data Monitoring System
- LDPC :- Low-Density Parity-Check
- LSA: Load Shed Application
- LDC:- Load Dispatch Center
- LT:- Low Tension
- MFT: Multifunction Transducers
- MMS: Manufacturing Message Specification
- MITM: Man-in-the-Middle
- MPLS : Multiprotocol Label Switching
- MPLS TP - Multi-Protocol Label Switching - Transport Profile
- MSP – Multiplex Section Protection
- MTS : Model Technical specification
- MTBF: Mean Time Between Failures
- MB: Mega Byte
- MCD: Momentary change Detection
- NOA:- Notification of Award
- NOI:- Notification of Intent
- NMS: Network Management system
- NEA- Nepal Electricity Authority
- NOC: Network Operation Center
- OA:- Optical Amplifier
- OADM- Optical Add Drop Multiplexer
- ODAR: Outage data analytics and reporting
- ODBC: Open Data Base Connectivity
- OEM: Original Equipment Manufacturer
- OFC: Optical Fiber Communication
- OFCS :-optical fiber Communications systems
- OPC: OLE for Process Control
- OPGW- Optical Ground Wire
- OLE:- Object Linking and Embedding
- OS: Operating System
- OSNR- Optical Signal-to-Noise Ratio
- OLTC: On-Load Tap Changer

- OTA: Over the Air
- OT- Operational Technology
- OTN- Optical Transport Network
- OUT:- Optical Transport Unit
- O&M: Operation & Maintenance
- PBG - Performance Bank Guarantee
- P2P :- Point-to-Point
- P2MP:- Point-to-Multipoint
- PLC: Programmable Logic Capabilities
- QAM:- Quadrature Amplitude Modulation
- QPSK:-Quadrature Phase Shift Keying
- RAM: Random Access Memory
- RDBMS: Relational database management system
- RDP – Remote Desktop Protocol
- REST:- Representational State Transfer
- ROADM - Reconfigurable Optical Add-Drop Multiplexer
- RTU: Remote Terminal Unit
- RTDB Real Time Database
- RF: Radio Frequency
- SAN: Storage area network
- SAT: Site Acceptance Test
- SCADA: Supervisory Control and Data Acquisition
- SCBO: Select Check Before Operation
- SDH: Synchronous Digital Hierarchy
- SLA: Service Level agreement
- SI: System Integrator
- SNCP – Sub Network Connection Protection
- SNTP: Simple Network Time Protocol
- SNMP: Simple Network Management Protocol
- SMF :- Single-mode fiber
- SMTP: Simple Mail Transfer Protocol
- SPOF:- Single Point Of Failure
- SRS:- System Requirements Specifications
- SS:- Substation
- SOA: Service-Oriented Architecture

- SOC: Security operation center
- SOE: Sequence of Events
- SOP: Safe Operating Procedures
- SQL: Structured Query Language
- SRV:- Stores Receipt Voucher
- S/S: Substations
- SSO: Single Sign On
- SSL: Secure Socket Layer
- S/W :- Software
- TCP/IP: Transmission Control Protocol/Internet Protocol
- TFT : Thin-Film Transistor
- TB: Tera Byte
- UAT:- User Acceptance Test
- UPS: Uninterrupted Power Supply
- URL: Uniform Resource Locator
- UDP: User Datagram Protocol
- VPS: Video Projection System
- VDU: Visual Display Unit
- VPN: Virtual Private Network
- XML: Extended Markup Language

Annexure: EMP Plan

Please find the Environmental Management Plan (EMP):

EMP.pdf

Table 1: Design Phase EMP

Topic	Activity / Issue	Commitment	Applicable Project Standards / Guidelines	Implementation Responsibility (Budget Source and Timing)	Monitoring Responsibility
Finalization of IEE	DC Gaps in baseline information and consultation required to inform detailed design	• Updating of the receptor inventory with results reflected in the updated IEE • Further meaningful consultations will be conducted as per the IEE	• ADB SPS (2009)	NEA NEA Counterpart Funds Before issue of bidding documents	NEA PMU / PISC
Siting and design of Project infrastructure	All Components Detailed design	• Design and layouts to reflect the requirements of the EMP and international engineering best practices/good EHS practice, as well as the issues raised by the public and other stakeholders as documented in the consultation chapter of the IEE report • Comply with all applicable national and state environment, health, and safety (EHS) regulatory requirements in addition to the mitigation measures set out in the EMP – if there is any conflict between national requirements and measures set out in the EMP the most stringent provisions will take precedence For all construction works undertake facilitated H&S risk assessment through a workshop during the design (and at other key stages) so it can inform both design and pre-construction preparations, considering both occupational and community H&S risks resulting from subsequent stages of the project. • Facilitated workshop will involve the design and construction team of the contractors and NEA operational staff.	• ADB SPS (2009) • IFC EHS General Guidelines • IFC EHS Electric Power T&D Guidelines • ILO Worker Accommodation[1] • GoN laws and regulations (Chapter 2 of IEE)	EPC Contractor Include in EPC contract cost Before design approval for further implementation during construction phase	NEA PMU / PISC

[1] 2https://www.ilo.org/media/340691/download

Topic	Activity / Issue	Commitment	Applicable Project Stanar Guidelines	Implementation Responsibility (Budget Source and Timing)	Monitoring Responsibility
	SCADA & Comm. Finalization of substation design and layout	• Design to minimize visual impact and clutter. Buildings will be designed in keeping with the existing substation buildings and/or local vernacular, albeit structurally sound etc. • Utilize landscape screening to screen the boundary wall and fences; these will need to be set back from the actual boundary to accommodate space for the vegetation. • In undertaking design, contractor with NEA to consult with communities in 500m of the site boundaries to get their views and input into the site layout (records of consultations are to be kept) • Designs will keep new impermeable surfaces to a minimum. • Cable trenches will be kept fully covered at all times to prevent H&S incident or small wildlife falling into them. • Design to provide spill prevention kits (sorbent pads, loose sorbent material, etc.) at storage areas and other at-risk locations within clearly labelled containers. • Locate new transformers; storage areas; and septic tanks/soak away at least 50m from waterbodies and borewells to reduce pollution risk, if closer proximity is required due to site layout further assessment to be carried out to demonstrate using a source-pathway-receptor model there will be no adverse impact on aquatic ecology or human health. • Septic tanks/soak aways will be placed away from drainage routes, waterlogged areas and shallow groundwater. • Internal access roads to be surfaced with asphalt or concrete. • Comply with Labour Accommodation Requirements appended to the IEE • For control buildings and other internal workspaces provide adequate natural and/or artificial lighting levels to meet the IFC EHS Guidelines on H&S (Table 2.3.3. Minimum Limits for Workplace Illumination Intensity) and take a life-cycle approach to detailed design, considering the use of construction materials and the energy and water efficiency of the building during operation adopting the "green building" concept e.g., using natural ventilation for reducing the need for air conditioners. Exhaust fans to be provided in kitchens and toilets. Detailed design is to include rainwater harvesting and enable NEA	• ADB SPS (2009) • IFC EHS General Guidelines • IFC EHS Electric Power T&D Guidelines • ILO Worker Accommodation[2] • GoN laws and regulations (Chapter 2 of IEE)	EPC Contractor Include in EPC contract cost Before design approval for further implementation during construction phase	NEA PMU / PISC

[2] 5https://www.ilo.org/media/340691/download

		to readily fit solar panels on building rooftop once operational. If solar panels are included in the scope they must not contain hazardous materials e.g., cadmium, lead, or selenium. Equipment purchased for use on the project is to be accompanied by letter from the manufacturer stating its composition and the leaching potential of any heavy metal content to determine if it is acceptable and how it is to be disposed on at end-of-life. Solar panels to have an anti-reflective coating to minimize glint and glare and maximize light absorption, racking to be anti-reflective. • Control building and other internal workspaces design will provide for sanitation and welfare facilities as per national regulations and international GIIP including indoor toilets with hand washing facilities (minimum of 1 unit to 6 males and 1 unit for 6 females shall be provided, it should not be necessary to go outside to use the toilets) connected to septic tank/soakaway and a dedicated cooking area with provision for non-wood cooking / clean eating area / rest area / segregated sleeping area for staff on-site etc. ILO worker accommodation guidelines to be followed - see annex on permanent accommodation provisions. • Dedicated shelter to be provided at the site entrance for use by security guards, shielding them from rain, wind, and extreme (hot / cold) temperatures. Separate accommodation will be provided for security guards on break. • All wastewater to be connected to existing sewerage system or septic tank with soak away so no untreated wastewater will be disposed of to surface water or ground in operation, septic tank/soakaway effluent to meet national general wastewater standards or IFC wastewater discharge limits, whatever is the most stringent. • Use of pit latrines and disposal of untreated sanitary wastewater is prohibited. • Design to ensure all lighting is of energy efficient LED type with solar powered LED lighting where practical Use of fluorescent/HPSV lamps will be avoided since they are less energy efficient/classed as hazardous waste for purposes of disposal. • Minimal outdoor lighting for H&S purposes to be installed to minimize disturbance to nocturnal wildlife. Outdoor lighting to be installed must be of low intensity with little or no blue wavelength and operated using passive infrared (PIR) technology movement sensors set at person height so as not to be kept permanently on overnight, it must be directional and shielded, so light does not fall outside substation boundaries. If lit externally buildings will be designed with non-reflective dark colored cladding materials to avoid reflecting light.			

		• Ensure conductors and/or jumpers are fitted with "bird sensitive" design measures e.g. adequate separation between live and ground or and insultation.			
	SCADA & Comm. Water supply	• Potable water will be supplied that meets national drinking water standards (full suite) as part of the design. • For on-site sources proposed undertake baseline water quality sampling per the EMoP to confirm suitability and as necessary design is to include additional water treatment, purification and storage facilities to facilitate safe drinking water supply. • Where a new drinking water supply for operation is required or additional water will be taken from an existing source the location, depth and other details of borewell to be informed by a detailed hydrogeological study also describing the availability of water taking into account climate change, mapping existing groundwater users, the current water abstraction rates and the additional volume of water required to be abstracted and the residual water balance at the end of the dry season. • Groundwater abstraction must avoid creating a water stress situation during the dry season for existing groundwater users and must ensure the baseflow of streams is not reduced. No groundwater will be used in locations without additional groundwater capacity – in other locations groundwater will only be used after it has been confirmed through assessment that there will be no additional stress on groundwater resources as a result. • If water supply is unavailable on site, ensure regular supply of bottled water meeting drinking water standards to be secured. • No groundwater will be used in locations without additional groundwater capacity – in other locations groundwater will only be used after it has been confirmed through assessment that there will be no additional stress on groundwater resources as a result	• ADB SPS (2009) • IFC EHS General Guidelines • GoN laws and regulations (Chapter 2 of IEE)	EPC Contractor Include in EPC contract cost Before design approval for further implementation during construction phase	NEA PMU / PISC

Topic	Activity / Issue	Commitment	Applicable Project Standards / Guidelines	Implementation Responsibility (Budget Source and Timing)	Monitoring Responsibility
	SCADA & Comm. Health and safety	• All electrical hazards will feature written and visual warning signs that meet the IEEE standards to include the ISO 7010 "Hazard Type: Electrical Symbol" warning of the risk of electrocution with an internal fence for high-risk equipment • Design to include lightening protection and earthing including earth mats in control buildings • Design of control building and other internal workspace to include emergency exits with emergency exit signage • Provide fully stocked, in-date first aid kit installed in a prominent, signed position, first aid posters and emergency contacts to also be displayed • Provide eye wash station and water supply to shower located near storage areas for fuel/oil/chemicals	• ADB SPS (2009) • IFC EHS General Guidelines/Occupational and Community Health and Safety • GoN laws and regulations (Chapter 2 of IEE)	EPC Contractor Include in EPC contract cost Before design approval	NEA PMU / PISC
	SCADA & Comm. Fire safety	• All substation buildings and other project facilities will be designed and constructed according to national fire safety standards, emergency response planning and response as well as international engineering best practice/good EHS practices • Separation walls or fire barrier walls shall be provided between the transformers and between transformer and nearby building. • Buildings including security cabin and high-risk locations outdoors to include smoke and/or heat detectors • Provide automatic fire alarm and fire suppression system in control building and at high-risk locations outdoors . • Provide sand buckets, full of sand, placed in a prominent, signed location near to fire-risk locations such as transformers and oil storage areas • Provide fire extinguishers (including for oil and electric fires) in a prominent, signed location in all buildings and security cabin and near to fire-risk locations such as transformers, DG sets, and oil storage areas with service and expiration dates clearly labelled along with posters on fire safety.	• ADB SPS (2009) • IFC EHS General Guidelines • IFC EHS Electric Power T&D Guidelines • GoN laws and regulations (Chapter 2 of IEE)	EPC Contractor Include in EPC contract cost Before design approval	NEA PMU / PISC
	SCADA & Comm. Access roads	• No new permanent access roads will be constructed.	• ADB SPS (2009)	EPC Contractor	NEA PMU / PISC

Environment, Health and Safety Codes of Practice

ENVIRONMENT

The national laws and regulations and IFC EHS guidelines should be followed along with the following environmental guidance:

Pollution Prevention

Air Pollution (Dust)

- Use of modern equipment, exclude over-aged or worn-out equipment or vehicles from the construction site
- Trucks importing loose raw materials or removing spoil must be covered with tarpaulin to reduce dust generation
- Position any stationary emission sources (e.g., water pumps, diesel generators, compressors, etc.) as far as practical from the nearest properties
- Impose speed limits on construction vehicles on off- and on-site access roads to minimize exhaust and dust emissions especially where access roads run adjacent to properties.
- Prohibit engine idling.
- Stockpiles of spoil and other dust generating materials to be kept to a minimum necessary to undertake works for the day and covered with tarpaulin.
- Minimize double handling and drop loads.
- Cover exposed soil with materials like gravel to minimize re-suspension of dust.
- Sprinkle earthworks, off- and on-site access roads that are not blacktopped, and material stockpiles with water during the construction period to avoid dust being dispersed by wind and mitigate dust related issues due to frequent movement of construction vehicles as necessary i.e., 2-3 times per day but more often if needed during excavations, dry and windy conditions that enable dust to be easily mobilized and the dust to be visible.
- Regularly clean dust from the off-site access roads during and immediately after construction work is completed.
- Strictly prohibit the burning of wastes generated by project-related activities.
- Ensure workers working near or having long exposure to vehicle exhausts and earthworks are provided with clean N95 dust masks to avoid inhalation or particulate matter and other pollutants.
- Periodic medical respiratory checks to be performed on workers exposed to high dust levels.

Noise and Vibration

- Use of modern equipment, exclude over-aged or worn-out equipment or vehicles from the construction site
- Select construction techniques and low noise generating equipment e.g., less than 55 dBA sound pressure level at 1m, and stage noisy works to limit their duration to minimize noise and vibration
- Fit all equipment and vehicles used in construction with exhaust silencers where the manufacturer’s design allows this
- Position any stationary emission sources (e.g., water pumps, diesel generators, compressors, etc.) as far as practical from the nearest properties
- Prohibit engine idling
- Prohibit use of horn by construction vehicles
- Impose speed limits on construction vehicles on off- and on-site access roads to minimize noise emissions especially where access roads run adjacent to properties
- Provide appropriate PPE (acoustic ear plugs or earphones capable of reducing noise levels to 80 dB(A) for hearing protection) to any workers subjected to noise levels of 80 dBA for more than 8 hours per day and ensure they wear it e.g., if piling etc.
- No unprotected ear should be exposed to a peak sound pressure level (instantaneous) of more than 140 dB(C) or average maximum sound levels of 110 dB(A).

- Periodic medical hearing checks to be performed on workers exposed to high noise levels of 80 dBA for more than 8 hours per day.

Soil and Water Pollution

- Avoid storage of all fuel, oil, and chemicals in areas located within 100m of surface water and groundwater springs, etc. to avoid direct contamination or contamination through run off
- Drums, containers or tanks of fuel, oil, or chemicals to be labelled and kept in a designated, labelled storage area under lock and key when not in use
- Establish dedicated fuel, oil, and chemicals stores (drums/containers/tanks) on impermeable bunded area of 110% volume to avoid spills and leaks contaminating soil and affecting water quality
- Secondary containment design to also consider means to prevent contact between incompatible materials in the event of a release.
- Place all drums or containers of fuel, oil, or chemicals on drip trays it not sited on impermeable surface with 110% bunded capacity.
- Place all equipment that containing fuel or oil on drip trays it not sited on impermeable surface with 110% bunded capacity.
- Undertake refilling or refueling only on areas of hard protected soil, preferably bunded, at least 100m from surface water with all drainage directed through oil interceptors.
- Provide drip trays/catch basins or other overflow/drip containment measures at connection points or possible overflow locations during refilling or refueling
- Use of dripless hose connections for vehicle tanks and fixed connections with storage tanks
- Use dedicated fittings, pipes, and hoses on containers or tanks and regularly inspect their condition
- Use of refilling or refueling equipment that is compatible and suitable for the characteristics of the materials being transferred and designed to ensure safe transfer
- Overfills of drums, containers, and tanks to be prevented as they are among the most common causes of leaks and spills resulting in soil and water contamination, this can be achieved by:
  - Checklist of measures to follow during filling operations
  - Provision of automatic fill shutoff valves to prevent overfilling
  - Installation of gauges on containers or tanks to measure volume inside
  - Use of pipe connections with automatic overfill protection (float valve)
  - Pumping less volume than available capacity by ordering less material than its available capacity
- Provision of overfill or over pressure vents that allow controlled release to a capture point
- Maintain procedures to prevent hazardous materials from being stored in incorrect containers or tanks
- Provide spill response kit with sufficient absorbent materials (e.g., sorbents, dry sand, sandbags) on-site for immediately soaking up any fuel, oil, or chemical leaks/spills that do accidentally occur
- Undertake construction during the dry season to minimize exposed areas subject to erosion by surface water runoff and to avoid flood risk, leading to accidents and/or water contamination.
- Deep excavations to be limited to dry season to prevent the need to pump out and dispose of sediment laden water.
- Works over or near watercourses will adopt protection measures to guard against loss of soil that would result in the turbidity of water.
- Implement measures to prevent landslides to avoid contamination of rivers by soil.
- Minimize soil erosion and surface water runoff by reducing the extent of earthworks, revegetating earthworks on completion, and covering stores of sand and spoil with tarpaulin
- Ensure surface water runoff from the construction site shall not discharge directly to surface water but shall be discharged through sedimentation basin and oil interceptor.
- Provision of oil-water separator on all drainage systems
- If water from excavations is pumped it must be disposed of via a sedimentation basin, it must not be disposed of directly to surface water.

- Do not allow washing of equipment or vehicles in surface water and ensure all washing water is discharged to sedimentation basin and oil interceptor instead of directly to surface water.
- Provision of designated hard standing areas for equipment servicing, refueling and wash down located at least 100m from surface water bodies, groundwater springs, with drainage directed through oil and grease interceptors before discharge into a settling pond
- Cement will be stored in enclosed storage facilities and not exposed to the elements.
- Do not undertake any concrete mixing within 100m of surface water
- Strict prohibition on open defecation and urination by construction workers
- No use of pit latrines
- Toilets and washing facilities to be connected to septic tank (with soak pit)
- No untreated wastewater is to be discharged direct to surface water or the ground
- Spent engine oil from the equipment will be collected and sent for recycling and re-use.

Materials and Waste Management

- Import all materials from existing licensed sources and keep records of all materials used, and sources.
- Storage yards will be fenced using a solid fence to catch windblown material.
- Minimize waste generation, restrict use of plastics and polyethene and use recyclable/biodegradable materials during construction to the extent possible
- Use durable, long-lasting materials that will not need to be replaced as often, thereby reducing the amount of construction waste generated over time.
- Purchase perishable construction materials e.g., paints incrementally to reduce spoilage of unused materials.
- Use building materials that have minimal packaging to avoid generation of excessive packaging waste
- Use construction materials containing recycled content when possible and in accordance with technical standards
- Prior to the start of works the contractor will ensure the waste management system is established at the construction sites and workers camps.
- Separate waste containers (drums, bins, skips or bags) will be provided for different types of waste; prevent the commingling or contact between incompatible wastes and allow for inspection between containers to monitor leaks or spills
- Sensitize workers on good housekeeping and the environmentally sound storage and disposal of construction and wastes, and importantly not to leave garbage lying around.
- Collect and segregate construction wastes including scrap metal, oil, and solid waste; ensure all workers are familiar with this segregation and arrange garbage bins to collect these wastes so they are not thrown on the floor
- Clearly identifying (label) and demarcating the waste storage area(s) on a site plan
- Store all the wastes produced in an environmentally sound manner in designated, labelled area with separate waste containers (drums, bins, skips or bags) for each distinct type of waste.
- Store solid waste in enclosed bins to contain leachate and avoid vermin.
- Store hazardous waste so as to prevent accidental releases to air, soil, and water resources in closed containers away from direct sunlight and rain
- Limiting access to hazardous waste storage areas to workers who have received proper training
- Secondary containment systems to be constructed using materials appropriate for the wastes being contained
- Provide adequate ventilation where volatile wastes are stored
- Conducting periodic inspections of waste storage areas and documenting the findings
- Encourage recovery of recyclable wastes that could be reused or sold to licensed recyclers, rather than disposing of it.
- Prohibit use of waste (e.g., empty cement bags and containers, plastic, wooden planks) for backfilling – only inert spoil may be used for backfilling to avoid need for off-site disposal (any excess inert spoil is to be disposed of at suitably licensed waste facilities).
- Prohibit burning of construction wastes.
- Prohibit dumping of construction wastes on-site, into streams, in agricultural fields etc.

- Provide weekly toolbox talk to remind of the importance of waste disposal, prohibition of disposal on the road, in drains etc., prohibition on burning of wastes, and open defecation and urination.
- Develop a procedure/system to penalize through escalating fines or similar any construction workers who breach these requirements.
  Document all wastes removed off site (including excavated soil, solid and hazardous waste) using transfer notes, to be taken by licensed waste contractors who should reuse/recycle or dispose of the waste to suitably licensed and engineered waste management facilities according to type
- Excavated spoil that cannot be reused to a licensed disposal site as suitable for accepting inert wastes ensuring no solid or hazardous wastes are comingled with the inert excavated spoil
- Collect solid waste and dispose of it to suitably engineered and licensed sanitary waste facilities
- Ensure any hazardous waste such as oily rags or old drums disposed of in suitably licensed hazardous waste facilities
- Waste containers designated for off-site shipment to be secured and labelled with the contents and associated hazards, be properly loaded on the transport vehicles before leaving the site, and be accompanied by a shipping paper, that describes the load and its associated hazards

Emergency Preparedness and Response Planning

1. For spills and leaks an emergency preparedness and response plan tailored to the hazards associated with the project, should include:

- SOP for the management of containment structures, specifically the removal of any accumulated fluid, such as rainfall, to ensure that the intent of the system is not accidentally or willfully defeated
- Implementation of inspection programs to ensure containment structures are physically intact and being well managed
- Identification of locations of hazardous materials and associated activities on an emergency plan
- Documentation of availability of specific personal protective equipment and training needed to respond to an emergency
- Documentation of availability of spill response equipment sufficient to handle at least initial stages of a spill and a list of external resources for equipment and personnel, if necessary, to supplement internal resources
- Description of response activities in the event of a leak, spill, release, or other emergency including internal and external notification procedures, specific responsibilities of individuals, decision process for assessing severity of the incident and determining appropriate action, first aid and emergency medical treatment, evacuation routes, post-event activities such as clean-up and disposal, incident investigation, worker re-entry, and replenishment of used PPE and spill response equipment
- Inspecting, testing, and maintaining the emergency response equipment
- Training of workers on release prevention, including drills specific to hazardous materials stored on site

Soil Erosion and Runoff Management

2. Bunding is an engineering soil conservation measure used for creating obstruction to the surface water runoff for controlling soil erosion. By bunding, an area is divided into smaller parts; thereby the effective slope length is reduced. The reduction of the slope length causes a reduction of the soil erosion as the surface runoff water is retained in the bund. Bunds are simple earthen embankments of varying lengths and heights, constructed across the slope. Graded bunds are adopted in case of high or medium annual rainfall (>600 mm) and relatively less permeable soil areas and in cases such as a construction site where the water ponded behind the bund is to be removed.

3. Construction of three-stage sedimentation ponds/tanks with an inlet, mid, and outlet section is required to allow sediment to settle out of surface water runoff before release of water. Silt fences can be used to channel surface water runoff to the sedimentation pond/tank. The working volume of the sedimentation pond/tank must be sufficient to allow for a minimum hydraulic retention time of at least 120 minutes under the peak surface water runoff conditions. If runoff rates exceed the capacity of a sedimentation pond/tank, one or more additional sedimentation ponds/tanks will be needed in parallel to accommodate the higher flow rates. Maximum sediment accumulation in the sedimentation pond/tank must be 25% or less.

HEALTH AND SAFETY

The national laws and regulations, IFC EHS guidelines, ILO safety and health in construction should be followed along with the following safety guidelines:

a. Preventive and protective measures should be introduced according to the following order of priority:

- Eliminating the hazard by removing the activity from the work process.
- Controlling the hazard at its source through use of engineering controls.
- Minimizing the hazard through design of safe work systems and administrative or institutional control measures.
- Providing appropriate personal protective equipment (PPE) in conjunction with training, use, and maintenance of the PPE.

b. OHS Training

- Training should generally be provided to management, supervisors, workers, and occasional visitors to areas of risks and hazards.
- Provisions should be made to provide OHS orientation training to all new employees to ensure they are apprised of the basic site rules of work at / on the site and of personal protection and preventing injury to fellow employees.
- Training should consist of basic hazard awareness, site- specific hazards, safe work practices, and emergency procedures for fire, evacuation, and natural disaster, as appropriate.
- Any site-specific hazard or color coding in use should be thoroughly reviewed as part of orientation training.

c. Basic OHS Training

- A basic occupational training program and specialty courses should be provided, as needed, to ensure that workers are oriented to the specific hazards of individual work assignments.
- Workers with rescue and first-aid duties should receive dedicated training so as not to inadvertently aggravate exposures and health hazards to themselves or their co- workers. Training would include the risks of becoming infected with blood–borne pathogens through contact with bodily fluids and tissue.
- Through appropriate contract specifications and monitoring, the contractor should ensure that service providers, as well as contracted and subcontracted labor, are trained adequately before assignments begin.

d. Tool Box Talks:

- Tool Box Talk meetings to be conducted every day before starting of the work. Work Plan for the day along with hazards/risks involved in the activities and safe working practices for the same are to be discussed with the workers, these can be conducted by contractor‘s supervisory staff as well.
- Record of the Tool Box Talk meeting to be generated and signature of all the workers/supervisor are to be taken on the meeting sheet. This activity will gradually enhance the safety awareness and will also help in operating in a planned manner.

e. Labeling

- All vessels that may contain substances that are hazardous as a result of chemical or toxicological properties, or temperature or pressure, should be labeled as to the contents and hazard, or appropriately color coded.

f. Noise

- No employee should be exposed to a noise level greater than 85 dB(A) for a duration of more than 8 hours per day without hearing protection. In addition, no unprotected ear should be exposed to a peak sound pressure level (instantaneous) of more than 140 dB(C).
- The use of hearing protection should be enforced actively when the equivalent sound level over 8 hours reaches 85 dB(A), the peak sound levels reach 140 dB(C), or the average maximum sound level reaches 110dB(A). Hearing protective devices provided should be capable of reducing sound levels at the ear to at least 85 dB(A).
- Although hearing protection is preferred for any period of noise exposure in excess of 85 dB(A), an equivalent level of protection can be obtained, but less easily managed, by limiting the duration of noise exposure. For every 3 dB(A) increase in sound levels, the 'allowed' exposure period or duration should be reduced by 50 percent.
- Prior to the issuance of hearing protective devices as the final control mechanism, use of acoustic insulating materials, isolation of the noise source, and other engineering controls should be investigated and implemented, where feasible

g. Electricity

- Marking all energized electrical devices and lines with warning signs
- Checking all electrical cords, cables, and hand power tools for frayed or exposed cords and following manufacturer recommendations for maximum permitted operating voltage of the portable hand tools
- Double insulating/grounding all electrical equipment used in environments that are, or may become, wet; using equipment with ground fault interrupter (GFI) protected circuits
- Appropriate labelling of service rooms housing high voltage equipment ('electrical hazard') and where entry is controlled or prohibited
- Conducting detailed identification and marking of all buried electrical wiring prior to any excavation work

h. Training and licensing industrial vehicle operators in the safe operation of specialized vehicles such as forklifts, including safe loading/unloading, load limits

- Ensuring drivers undergo medical surveillance
- Ensuring moving equipment with restricted rear visibility is outfitted with audible back-up alarms
- Establishing rights-of-way, site speed limits, vehicle inspection requirements, operating rules and procedures, and control of traffic patterns or direction
- Restricting the circulation of delivery and private vehicles to defined routes and areas, giving preference to 'one-way' circulation, where appropriate

i. Fall prevention and protection measures should be implemented whenever a worker is exposed to the hazard of falling more than two meters. Fall prevention may include:

- Installation of guardrails with mid-rails and toe boards at the edge of any fall hazard area

- Proper use of ladders and scaffolds by trained employees
- Use of fall prevention devices, including safety belt and lanyard travel limiting devices to prevent access to fall hazard area, or fall protection devices such as full body harnesses used in conjunction with shock absorbing lanyards or self- retracting inertial fall arrest devices attached to fixed anchor point or horizontal lifelines
- Appropriate training in use, serviceability, and integrity of the necessary PPE
- Inclusion of rescue and/or recovery plans, and equipment to respond to workers after an arrested fall

j. Fires and or explosions resulting from ignition of flammable materials or gases can lead to loss of property as well as possible injury or fatalities to project workers. Prevention and control strategies include:

- Storing flammables away from ignition sources and oxidizing materials.
- Defining and labeling fire hazards areas to warn of special rules (e.g. prohibition in use of smoking materials, cellular phones, or other potential spark generating equipment);
- Providing specific worker training in handling of flammable materials, and in fire prevention or suppression

k. Personnel Protective Equipment

- Risks to the health and safety of workers can be prevented by provision of Personal Protective Equipment (PPEs) to all workers. Personal protective equipment like safety gloves, helmet, mufflers etc. will be provided during the construction period and during the maintenance work. This will be included in the BOQ list. Depending on the nature of work and the risks involved, contractors must provide without any cost to the workers, the following protective equipment. The list of protective equipment is given in Table 1.
- Helmet shall be provided to all workers, or visitors visiting the site, for protection of the head against impact or penetration of falling or flying objects.
- All PPE must be of good quality with mark of quality standard certification.
- Safety belt shall be provided to workers working at heights for bridge construction, etc.
- Safety boots shall be provided to all workers for protection of feet from impact or penetration of falling objects on feet.
- Ear protecting/ earmuffs/plugs shall be provided to all workers in high noise zones.
- Eye and face protection equipment shall be provided to all welders to protect against sparks.
- Respiratory protection devices shall be provided to all workers during occurrence of fumes, dusts, or toxic gas/vapor.
- The supervisor must ensure that appropriate personal protective equipment is available to workers; properly worn when required and properly cleaned, inspected, maintained and stored.
- A worker shall be responsible for using the items of personal protective equipment provided by the employer;
- A worker who is required to use personal protective equipment must-
    - Use the equipment in accordance with training and instruction.
    - Inspect the equipment before use.
    - Refrain from wearing protective equipment outside of the work area which if done so would constitute a hazard; and
    - Report any equipment malfunction to the supervisor or employer.
- A worker who is assigned responsibility for cleaning, maintaining or storing personal protective equipment must do so in accordance with training and instruction provided.
- An emergency procedures manual will be kept.

- First aid facilities will be made available on-site and doctors called in from nearby village/towns when necessary. Minimum contents of the first aid box is given in Table 2.

Table 1 - Personnel Protection Equipment (PPE) for safety of different body parts

No.	Body Part to be Protected	PPE
1	Head	Safety helmet, hard hat, Crash helmets
2	Eye	Eye protectors, eye protectors for radiations, shield and helmet, zero power goggles
3	Ear	Earplug, earmuffs
4	Noise-Mouth	Du respirator, gas mask, self-contained breathing apparatus, dust masks
5	Hand	Standard work gloves, cutting gloves, leather work gloves, heat protective gloves, anti-vibration gloves
6	Foot	Industrial safety boots, chemical-proof boots
7	Body	Standard work clothing, chemical-proof clothing, heat protective clothing, leather apron
8	Others	Safety belts, personal protective equipment for radiation protection, back support belts
9	Communicable diseases	Sanitizer, masks etc.

Table 2 - Contents of first-aid box

Sr. No.	Description	Quantity
1	First aid leaflet	1 copy
2	Sterilized finger dressing	10 nos.
3	Sterilized hand or foot dressing	10 nos.
4	Sterilized body or large dressing	6 nos.
5	Sterilized burns dressing - small	4 nos.
6	Sterilized burns dressing - large	2 nos.
7	Sterilized burns dressing – extra large	6 nos.
8	Sterilized cotton wool (25 gms)	2 tubes
9	Cetavolon	2 tubes
10	Eye pads	6 nos.
11	Adhesive plaster	1 spool
12	Assorted roller bandage	6 nos.
13	Triangular bandages	6 nos.
14	Safety pins	6 nos.
15	Scissors, ordinary, 12.7cms, both sides sharp	1 pair
16	Antiseptic liquid, 150 ml, or equivalent	2 nos.
17	Cotton wool for padding, 100 gms	2 packets
18	Eye Ointment of sulphacetamide preparation	1 tube
19	Loose woven gauze (28”x8”), compressed pack	1 packet
20	Aspirin, 300 mg (10 tablets)	5 strips
21	Note Pad, with a pencil in a plastic cover	1 no.
22	Adhesive dressing strips	10 strips
23	Field dressing of modified army pattern	3 nos.
24	Record cards in a plastic cover	1 set
25	Torch, medium size	1 no.
26	Eye wash	1 no.

Sr. No.	Description	Quantity
27	Wooden splints, small	1 set
28	Wooden splints, big	1 set
29	Disinfectant, Spirt, 100ml	1 bottle

l. Proper demarcation & barricading

Safety barricading to be done around the working area from day one to safeguard against trespassing. —people at work board must be placed to indicate work under progress in the vicinity. Barricading to be kept in place till the work is over, even if it takes few days to complete. No excavated pits / loose soil areas should be kept open without barricading around the area. Also, all storage area of materials near the working area must be demarcated and barricaded properly.

m. Use of cranes

- Cranes with 20% factor of safety (i.e. cranes with a lifting capacity higher than the weight to be lifted) are to be used.
- The crane should be operated by a licensed operator only.
- Operational fitness of the crane has to be checked before hiring the crane.
- The lifting hooks must have a safety lock in place to avoid slipping of the clings.
- The lifting capacity of the slings to be checked before starting of the work. The slings with 20% factor of safety in mechanical strength must be used for lifting.

n. Working near the existing power lines:

- No work to be taken up without proper shutdown while working in the existing power line or while working in the proximity of any existing power line.
- Work to be started only after the line (all the phases) is properly/securely earthed from both the ends and line clearance/work permit is issued by the concerned authority in writing with start and end time specifically mentioned.
- All the earthing points to be personally verified by senior engineer of contractor as EHS supervisor. Also secure against re-connection.
- No shutdown to be arranged over phone communication. Personal check is to be made for every shutdown and line clearance.
- The work under shutdown should be executed under direct supervision of a qualified supervisor/engineer of NEA and the owner (if not NEA line). The work group should not be left alone to execute the work.

o. Material handling & work process:

- Poles and accessories to be stored in proper demarcated area and should be away from the routes/places of public use.
- Ensure adequate ingress & egress around the work area.
- While lifting or shifting the equipment nobody should stay boarded.
- Correct tools and plant must be used for fixing and assembling to avoid accidents in the process. All the work must be supervised by senior engineer of contractor as EHS supervisor who can guide the team in every activity.

- While lifting heavy items with multiple sections, proper support slings (along the length) are to be provided from the point of lifting sling to the bottom of the item to avoid fall of sections due to malfunction of the slip joints.
- No persons under the influence of alcohol neither be allowed to enter the work location nor should help in the work from outside by any means.

p. Records and documentation

Reports prepared by the contractor shall include information on the place, date and time of the incident, name of persons involved, cause of incident, witnesses present and their statements. Based on such reports, the management can jointly identify any unsafe conditions, acts or procedures and recommend for the contractor to undertake certain mitigative actions to change any unsafe or harmful conditions.

q. Accidents and Diseases monitoring: the contractor should establish procedures and systems for reporting and recording:

- Occupational accidents and diseases
- Dangerous occurrences and incidents

These systems should enable workers to report immediately to their immediate supervisor any situation they believe presents a danger to life or health. The systems and the employer should further enable and encourage workers to report to management all:

- Occupational injuries and near misses
- Suspected cases of occupational disease
- Dangerous occurrences and incidents

All reported occupational accidents, occupational diseases, dangerous occurrences, and incidents together with near misses should be investigated with the assistance of a person knowledgeable/competent in occupational safety. The investigation should: Establish what happened; Determine the cause of what happened, identify measures necessary to prevent a recurrence, Distinction is made between fatal and non-fatal injuries. These two main categories are divided into three sub-categories according to time of death or duration of the incapacity to work.

OHS Plan will include:

1. Safety Training Program – to provide general and specialized training courses for all workers on the site and at all levels of supervision and management. General courses will consist of (i) an initial Safety Induction which all workers will be required to attend prior to being allowed to work on site, all visitors and project workers who have not attended the safety induction course must be always accompanied by inducted workers when within the working area. and (ii) periodic safety training refreshers covering similar topics to induction, conducted not less than once every six months. All subcontractor workers will be required to participate in relevant training courses appropriate to the nature, scale, and duration of the subcontract. Since they have heightened risk only trained workers must undertake certain activities e.g., working at height, working in confined spaces, working with electricity etc. Workers must have attended such training before they are involved in relevant works and the contractor must either offer an internal training course or organize for attendance on an external specialist training course. Workers must have a training record of attending a suitable training course. Untrained workers will not be permitted to work at height, enter confined spaces, work with live electricity etc.

2. Medical Check-Up/Health Surveillance – of workers fitness, eyesight, hearing, respiratory health, and communicable and noncommunicable diseases before work commences; and then repeated every six months by the contractor during construction. Only workers who have passed their fitness test and have the requisite medical clearance must undertake certain activities e.g., working with electricity etc.

3. Safety Meetings – will be conducted monthly during construction phase by APDCL. During construction the meetings will require attendance by the safety representatives of all contractors and subcontractors on-site. The minutes of all safety meetings including actions agreed will be taken and sent to APDCL within seven days of the meeting.

4. Safety Inspections – the contractor will regularly inspect, test, and maintain all safety equipment, scaffolds, guardrails, working platforms, hoists and other lifting equipment, ladders and other means of access, lighting and signage, firefighting equipment, first aid kit, stock take and condition of PPE etc. Signs will be graphic and in the languages of workers, kept clear of obstructions and legible to read. Lighting will meet illumination guidelines for the working area as per IFC EHS Guidelines on OHS. Equipment, which is damaged, dirty, incorrectly positioned or not in working order will be immediately repaired, or replaced, by the contractor.

5. Site Audit - during construction the contractor's H&S officer and APDCL will undertake monthly audits of compliance with the health and safety plan.

6. Personal Protective Equipment (PPE) as a last resort where risks cannot be avoided – workers will be provided (before they start work) with appropriate PPE at no cost to the workers. PPE provided to workers (regardless formal and informal, directly contracted or subcontracted) in accordance with GoN legislation and Table 2.7.1. Summary of Recommended Personal Protective Equipment according to Hazard in IFC EHS Guidelines on OHS including safety shoes, helmets, goggles, earmuffs, and face masks and ensure that this is always worn by them with a strict disciplinary system (no work condition if not compliant) being enforced for any non-compliance.

7. Work Zone Noise Levels: during construction protective measures need to be provided and as per the WB-IFC EHS Guidelines on OHS, Table 2.3.1. sets the level at 85 dB (A) for 8 hours exposure this being more stringent than the GoN requirements will be adopted, as well as 140 dB(C) peak/instantaneous noise exposure for workers working near the high noise generating machinery. High noise work areas must be adequately signposted. In these high noise work areas PPE in the form of sound reducing earmuffs/ear plugs to the workers are to be provided. In the first instance, however, reduction in noise levels to the lowest practical level must be achieved by adoption of suitable preventive measures, such as, use of enclosures with suitable absorption material, etc. Workers operating in the high noise work areas will be given auditory tests as part of health surveillance.

8. EMF levels at the construction site to be kept within international good practice levels as per ICNRP (reference and peak values) for the occupational exposure.

9. Electricity: IFC EHS Guideline on Electric Power Transmission and Distribution requirements for working with electricity will be observed with only licensed electricians that meet the requirements set out in them allowed to work on live electricity with strict adherence to safety standards including those listed in said guidelines. Live lines will be deactivated and properly grounded before work is performed on, or in proximity, to the lines and this will be checked and certified in writing by the contractor's Health and Safety Officer in advance. While working at heights personal safety measures such as harnesses, tool bags, ropes etc. will need to be provided.

10. Emergency Preparedness and Response Sub-Plan including communication systems and protocols to report an emergency e.g., health emergency, work-related accident including electrocution, traffic accident, accident involving the community, natural hazard including flooding, fire, virus outbreak etc. It will need to be developed in consultation with local emergency services with adequate fire and first aid first-responders will need to be based on the construction site

to facilitate immediate response. Provide readily available first aid for workers as well as an ambulance for more serious cases. Make arrangements for a doctor on call and nearest Health Center and/or Hospital for emergency cares of workers. Regular drills will be required involving all workers to prepare for an incident.

11. International good practice measures provided in the IFC EHS Guidelines: https://www.ifc.org/en/insights-reports/2000/general-environmental-health-and-safety-guidelines and ILO Safety and Health in Construction (2022): https://www.ilo.org/resource/other/safety-and-health-construction-revised-edition

Labor Accommodation Requirements

Temporary Worker Accommodation

In addition to GON requirements for temporary overnight labor accommodation follow ILO Safety and Health in Construction and worker accommodation guidelines and the below points to comply with the core labor standards etc.

Day camps with temporary structures to provide protection against the weather conditions for rest and eating of food will be required at site as a rest area but these are not to be used for sleeping overnight. Adequate quantity of safe drinking water and container for their safe storage shall be provided at day camps; at least 4 liters of water per person per day to be provided for consumption during the working day at each site. If no existing toilets within 100m that can be used, temporary sanitation facilities for men and women workers shall be provided where the wastewater generated is enclosed in a container to be later taken offsite for wastewater treatment and disposal. Food provided to day camps should be cooked off site; if it is to be reheated at site fire-safety measures must be adopted with LPG cylinders or kerosene purchased from authorized vendors. After completion of the construction work the temporary structures shall be removed and the land will be restored to its earlier condition.

1.1 General living facilities

Location

- Appropriate siting to avoid flooding or other natural hazards
- Location within a reasonable distance from the worksite to be unaffected by the worksite's noise, emissions or dust but avoiding undue amount of time travelling to work
- Safe and free transport to the worksite where remotely located
- Built with structurally sound materials, kept in good repair, clean and free from rubbish and other refuse
- After completion of the construction work the temporary structures shall be removed and the land will be restored to its earlier condition.

Drainage

- Adequate drainage, no waterlogging

Heating, air conditioning, ventilation and light

- Adequate heating, air conditioning and ventilation where appropriate
- Adequate natural light and artificial light, including emergency lighting

Water

- Easy access to an adequate supply of free, safe and potable water
- Constructed and covered storage tanks to prevent water from pollution or contamination
- Regular monitoring of drinking water quality

Wastewater and solid waste

- Adequate discharge of wastewater, sewage, food and any other waste materials
- Disposal of sewage and other wastewater shall be made connected to an existing sewerage system or made through a septic tank-soak pit arrangement
- Separate enclosed (lidded) bins with proper markings in terms of recyclable or non-recyclable waste shall be provided in the labor camps and kitchen premises in sufficient numbers for collection of garbage.
- Specific containers for rubbish collection in adequate number and being regularly emptied
- Pest extermination, vector control and disinfection throughout the living facilities

1.2 Rooms/dormitories facilities

- Kept in good condition, aired and cleaned at regular intervals
- Built with easily cleanable flooring materials
- Adequate furniture (such as table, chair, mirror, bedside light) for every worker
- Lockable doors and windows with mosquito screens when necessary
- Living space and space for privacy
- Adequate living space (see also International standards for spacing at migrant workers' accommodation)
- Adequate headroom, providing full and free movement, of not less than 203 cm
- Inside dimensions of a sleeping space of at least 198 cm by 80 cm
- Minimized number of workers sharing the same room/dormitory (recommended 2–8 worker)
- Mobile partitions or curtains to ensure privacy
- Gender-segregated accommodations, except in family accommodation
- Separate sleeping rooms for shifts to ensure no workers working during the day share a room with workers on night shifts
- Bed arrangements and storage facilities
- A separate bed for each worker
- Minimum space of 1 m between beds
- Minimized use of double deck bunks and no use of triple deck bunks
- Enough clear space between the lower and upper bunk of the bed where double deck bunks are in use (recommended 0.7–1.1 m)
- Reasonably comfortable bedding materials (mattress, pillow, cover and clean bed linen) for each worker
- Bedding and bedframe materials designed to deter vermin
- Individual, lockable storage facilities for each worker to secure their belongings

1.3 Sanitary facilities

- Sanitary and toilet facilities provided for men and women including private bathing area, showers, or baths in overnight accommodation.
- Separate housekeeping staff shall be engaged for regular cleaning of the accommodation.
- Frequent cleaning and kept in good condition
- Located within the same buildings with rooms/dormitories
- Constructed from easily cleanable materials
- Shower/bathroom flooring made of anti-slip hard washable materials

- Adequate privacy, including ceiling to floor partitions and lockable doors
- Adequate number of sanitary facilities (a minimum of one toilet, one wash basin and one tub or shower for every six persons)
- Convenient and easily accessible location
- Compliance with minimum standards of health and hygiene
- Separate sanitary facilities for men and women, except in family accommodation
- Suitable light and good ventilation to open air, independently of any other part of the accommodation
- Adequately stocked soap and hygienic paper
- Adequate supply of hot and cold fresh running water (at least 80-100 liters per capita per day)

1.4 Canteen, cooking and laundry facilities

- If workers cook their own meals, kitchen space is provided separately from the sleeping areas.
- No labor shall be allowed to collect fuel wood/NTFP or purchase fuel wood/NTFP from unauthorized vendors.
- LPG cylinders or kerosene purchased from authorized vendors shall be provided.
- Being built with adequate and easy to clean materials
- Being kept in clean and sanitary condition
- Common dining rooms, canteens or mess rooms, and kitchen space located away from sleeping areas
- Enough space in the canteen (1–1.5 m2 per worker)
- Adequately furnished canteen (tables, benches, individual drinking cups and plates)
- Adequate facilities to maintain adequate personal hygiene (enough washbasins, clean water, materials for hygienic drying)
- Places for food preparation adequately ventilated and equipped to protect against contamination between and during food preparation
- Kitchen floor, ceiling and wall surfaces adjacent to or above food preparation and cooking areas built in non-absorbent, durable, non-toxic, easily cleanable materials
- Wall surfaces adjacent to cooking areas made of fire-resistant materials; food preparation tables equipped with a smooth, durable, non-corrosive, non-toxic, washable surface
- Adequate facilities for cleaning, disinfecting and storage of cooking utensils and equipment
- Adequate sealable containers to deposit food waste and other refuse; refuse frequently removed from the kitchen to avoid accumulation
- Implementation of the WHO “5 keys to safer food” or equivalent process in relation to food safety
- Provided food containing appropriate nutritional value and considering migrant workers' religious/cultural backgrounds
- Adequate facilities for washing and drying clothes, appropriately situated and furnished laundry facilities
- Collection of waste water from washing areas and kitchens further disposed through existing sewerage connection or septic tank with soak away

Medical facilities

- Adequate number and stock of first aid kits
- Adequate number of staff/workers trained to provide first aid
- Residents are provided guidance on alcohol, drug and HIV/AIDS and other health risks
- On site medical facilities/services (where possible and depending on the medical infrastructure existing in the community)
- Separate facilities for sick workers to prevent the spread of transmissible diseases among occupants

- Appropriate and reasonable accommodations in connection with pregnancy, childbirth and nursing

1.6 Leisure, social and telecommunication facilities

- Basic collective social/rest spaces and adequate recreational areas where not otherwise available in the community
- Dedicated places for religious observance
- Reasonable access to internet facilities, telephone or other modes of communications free of charge or at affordable/public prices

2.1 Management and staff

- An appointed person with adequate background, competency and experience to manage the accommodations or monitor third-party service providers
- Clear contractual management responsibilities and monitoring and reporting requirements where third-party service providers are being used
- Adequate staff to implement the accommodation standards (cleaning, cooking, security, general maintenance)
- Basic health and safety training for staff, including training in nutrition and food handling for those in charge of the kitchen
- Frequent inspection and maintenance of premises and records kept

2.2 Fees and costs for accommodation and related services

- Accommodation free of charge where migrant workers are not free to look for their own accommodations
- Fair and transparent renting arrangements, not costing migrant workers more than a small proportion of income (when costs are charged)
- Adequate information to migrant workers about all payments made
- Clearly specifying renting arrangements and regulations in migrant workers' employment contracts
- Food and other services provided at the facilities for free or reasonably priced (this means not above the local market price)
- No in-kind payments for accommodation and related services

2.3 Health and safety

- Adequate health and safety management plans including electrical, mechanical, structural and food safety
- Available emergency plans on health and fire safety and other specific occurrences (earthquakes, floods, tornadoes, pandemic)
- Regular training in safety and health rules and procedures for all occupants
- Posting of safety notices and operational instructions in language migrant workers understand or visual form
- Adequate number of staff/workers trained in providing first aid
- Easy access to medical facilities and medical staff, including women doctors/nurses where appropriate Guidance on alcohol, drug and HIV/AIDS and other health risks-related activities provided to migrant workers
- Access to adequate contraception measures and mosquito nets (where relevant)

Fire safety

- Specific and adequate fire safety plan and measures
- Training of fire wardens
- Installing, periodic testing and maintenance of fire equipment (alarms, extinguishers, etc.)
- Training for migrant workers in fire procedures and periodic drills (in a language they understand)
- Bedding not containing flammable materials
- Radiators and other heating apparatus properly placed to avoid risk of fire, and shielded where necessary to prevent discomfort to occupants
- Emergency evacuation plans are displayed at strategic areas in language understood by workers
- Clearly marked emergency exits
- Adequate means of escape provided and properly maintained

2.4 Security

- Security at worker's accommodation shall be ensured.
- A security plan including clear measures to protect migrant workers against theft and attack and clear provisions on the use of force
- The backgrounds of security staff checked for previous crimes or abuses
- Clear instructions for security staff not to harass, intimidate, discipline, discriminate against migrant workers or restrict the freedom of movement
- Adequate training for security staff in dealing with violence and harassment and the use of force (including gender-based violence and sexual harassment)
- Body searches only performed in exceptional circumstances by specifically trained security staff; pat down searches on women workers only performed by women security staff

2.5 Migrant workers' rights, rules and regulations on migrant workers' accommodation

- Migrant workers' 24/7 access to the accommodation; security measures reasonable and not unduly restricting migrant workers' freedom of movement
- Adequate transport system to the surrounding communities
- Withholding migrant workers' documentation papers prohibited; migrant workers entitled to keep their documents in their own lockers
- Trade union representatives' access to migrant workers in the accommodation site
- Visitor access allowed in accordance with company rules for privacy or safety
- Migrant workers' religious, cultural and social backgrounds respected
- Adequate information to migrant workers about their rights and obligations (a copy of the accommodations' internal rules, procedures and sanction mechanism in a language or through a media they understand)
- Non-discriminatory, fair and reasonable house regulations
- Effective grievance mechanisms for migrant workers to articulate their grievances
- Display of contact information of consular services, company personnel and civil society organizations at the facilities

Permanent Worker Accommodation

In addition to GON requirements for permanent labor accommodation follow ILO worker accommodation guidelines and the below additional points to comply with the core labor standards etc.

Integrity of Structures

- Surfaces, structures and installations should be easy to clean and maintain, and not allow for accumulation of hazardous compounds.
- Buildings should be structurally safe, provide appropriate protection against the climate, and have acceptable light and noise conditions.
- Fire resistant, noise-absorbing materials should, to the extent feasible, be used for cladding on ceilings and walls.
- Floors should be level, even, and non-skid.

Severe Weather

- Structures should be designed and constructed to withstand the expected elements for the region and have an area designated for safe refuge, if appropriate.

Exit

- Passages to emergency exits should be unobstructed at all times.
- Exits should be clearly marked to be visible in total darkness. The number and capacity of emergency exits should be sufficient for safe and orderly evacuation of the greatest number of people present at any time, and there should be a minimum of two exits from any work area.
- Facilities also should be designed and built taking into account the needs of disabled persons.

Fire Precautions

- Equipping facilities with fire detectors, alarm systems, and fire-fighting equipment. The equipment should be maintained in good working order and be readily accessible. It should be adequate for the dimensions and use of the premises, equipment installed, physical and chemical properties of substances present, and the maximum number of people present.
- Provision of manual firefighting equipment that is easily accessible and simple to use
- Fire and emergency alarm systems that are both audible and visible

Lavatories and Showers

- Adequate lavatory facilities (toilets and washing areas) should be provided for the number of people expected to work/live in the facility and allowances made for segregated facilities, or for indicating whether the toilet facility is “In Use” or “Vacant”. Toilet facilities should also be provided with adequate supplies of hot and cold running water, soap, and hand drying devices.

Potable Water Supply

- Adequate supplies of potable drinking water should be provided from a fountain with an upward jet or with a sanitary means of collecting the water for the purposes of drinking
- Water supplied to areas of food preparation or for the purpose of personal hygiene (washing or bathing) should meet drinking water quality standards

Lighting

- Workplaces should, to the degree feasible, receive natural light and be supplemented with sufficient artificial illumination to promote workers' safety and health, and enable safe equipment operation. Supplemental 'task lighting' may be required where specific visual acuity requirements should be met.
- Emergency lighting of adequate intensity should be installed and automatically activated upon failure of the principal artificial light source to ensure safe shut-down, evacuation, etc.

Safe Access

- Passageways for pedestrians and vehicles within and outside buildings should be segregated and provide for easy, safe, and appropriate access
- Equipment and installations requiring servicing, inspection, and/or cleaning should have unobstructed, unrestricted, and ready access
- Hand, knee and foot railings should be installed on stairs, fixed ladders, platforms, permanent and interim floor openings, loading bays, ramps, etc.
- Openings should be sealed by gates or removable chains
- Covers should, if feasible, be installed to protect against falling items
- Measures to prevent unauthorized access to dangerous areas should be in place

First Aid

- Ensure that qualified first-aid can be provided at all times.
- Appropriately equipped first-aid stations should be easily accessible throughout the place of work
- Eye-wash stations and/or emergency showers should be provided close to all workstations where immediate flushing with water is the recommended first-aid response
- Where the scale of work or the type of activity being carried out requires, dedicated and appropriately equipped first-aid room(s) should be provided. First aid stations and rooms should be equipped with gloves, gowns, and masks for protection against direct contact with blood and other body fluids
- Remote sites should have written emergency procedures in place for dealing with cases of trauma or serious illness up to the point at which patient care can be transferred to an appropriate medical facility.

Air Supply

- Sufficient fresh air should be supplied for indoor and confined work spaces. Factors to be considered in ventilation design include physical activity, substances in use, and process- related emissions.
- Air distribution systems should be designed so as not to expose workers to draughts
- Mechanical ventilation systems should be maintained in good working order. Point-source exhaust systems required for maintaining a safe ambient environment should have local indicators of correct functioning.
- Re-circulation of contaminated air is not acceptable. Air inlet filters should be kept clean and free of dust and microorganisms.
- Heating, ventilation and air conditioning (HVAC) and industrial evaporative cooling systems should be equipped, maintained and operated so as to prevent growth and spreading of disease agents (e.g. Legionella pneumophilia) or breeding of vectors (e.g. mosquitoes and flies) of public health concern.

Temperature

- The temperature in work, rest room and other welfare facilities should, during service hours, be maintained at a level appropriate for the purpose of the facility.

OHS Training

- Provisions should be made to provide OHS orientation training to all new employees to ensure they are apprised of the basic site rules of work at / on the site and of personal protection and preventing injury to fellow employees.
- Training should consist of basic hazard awareness, site- specific hazards, safe work practices, and emergency procedures for fire, evacuation, and natural disaster, as appropriate. Any site-specific hazard or color coding in use should be thoroughly reviewed as part of orientation training.

Permanent Accommodation

- A separate bed for each worker
- Adequate headroom, providing full and free movement, of not less than 203 cm
- The minimum inside dimensions of a sleeping space should be at least 198 cm by 80 cm
- Beds should not be arranged in tiers of more than two
- Bedding materials should be reasonably comfortable
- Bedding and bedframe materials should be designed to deter vermin
- Separate accommodation of the sexes
- Adequate natural light during the day- time and adequate artificial light
- A reading lamp for each bed
- Adequate ventilation to ensure sufficient movement of air in all conditions of weather and climate
- heating where appropriate
- Adequate supply of safe potable water
- Adequate sanitary facilities (see below)
- Adequate drainage
- Adequate furniture for each worker to secure his or her belongings, such as a ventilated clothes locker which can be locked by the occupant to ensure privacy
- Common dining rooms, canteens or mess rooms, located away from the sleeping areas
- Appropriately situated and furnished laundry facilities
- Reasonable access to telephone or other modes of communications, with any charges for the use of these services being reasonable in amount
- Rest and recreation rooms and health facilities, where not otherwise available in the community
- In workers' sleeping rooms the floor area should not be less than 7.5 square metres in rooms accommodating two persons; 11.5 square metres in rooms accommodating three persons; or 14.5 square metres in rooms accommodating four persons. If a room accommodates more than four persons, the floor area should be at least 3.6 square metres per person. Rooms should indicate the permitted number of occupants.
- As far as practicable, sleeping rooms should be arranged so that shifts are separated and that no workers working during the day share a room with workers on night shifts.

Sanitation Facilities

- Adequate sanitary facilities should include a minimum of one toilet, one wash basin and one tub or shower for every six persons. They should be provided at a convenient location which prevents nuisances.
- Sanitary facilities provided should meet minimum standards of health and hygiene. They should also provide reasonable standards of comfort, including hot and cold fresh running water.
- There should be separate sanitary facilities provided for men and for women.
- Sanitary facilities should have ventilation to the open air, independently of any other part of the accommodation.

- Soap and hygienic paper should be adequately stocked.
- Measures should be taken to prevent the spread of diseases. Separate facilities should be provided for sick workers to prevent the spread of transmissible diseases among the occupants.
- Fire safety measures should be taken, including installing and maintaining fire equipment (alarms, extinguishers, etc.).
- Workers should be trained in fire procedures.
- Bedding should not contain flammable materials.
- Radiators and other heating apparatus should be placed so as to avoid risk of fire, and shielded where necessary to prevent discomfort to occupants.

Inspection of premises

- Premises should be inspected frequently to ensure that the accommodation is clean, decently habitable and maintained in a good state of repair. The results of each such inspection should be recorded and be available for review.

Vacating the premises upon termination of employment

- When a worker's contract of employment is terminated, the worker should be entitled to a reasonable period of time to vacate the premises, in accordance with national law and custom.

Water Conservation

- Regularly maintain plumbing, and identify and repair leaks
- Shut off water to unused areas
- Install self-closing taps, automatic shut-off valves, spray nozzles, pressure reducing valves, and water conserving fixtures (e.g. low flow shower heads, faucets, toilets, urinals; and spring loaded or censored faucets)
- Operate dishwashers and laundries on full loads, and only when needed
- Install water-saving equipment in lavatories, such as low- flow toilets

NEPAL ELECTRICITY AUTHORITY

(An Undertaking of Government of Nepal)
Project Management Directorate
Distribution Line and Substation Department

NEA DIGITAL NETWORK AND SCADA EXPANSION PROJECT

BIDDING DOCUMENT
FOR

Procurement of Plant for
Design, Supply, Installation and Commissioning
of
NEA Digital Network and SCADA Expansion

(Procurement of Plant)

Single-Stage, Two-Envelope
Bidding Procedure

Issued on:	**22nd February 2026**
Invitation for Bids No.:	**PMD/ETDSP/NDNSEP-082/83-01**
OCB No.:	**PMD/ETDSP/NDNSEP-082/83-01**
Employer:	**Nepal Electricity Authority**
Country:	**Nepal**

VOLUME –II (Part-B)

NEA Digital Network & SCADA Expansion Project
Distribution Line and Substation Department
Project Management Directorate
Matatirtha, Kathmandu, Nepal
Telephone: 01 5164099

(Volume -II, Part-B)
Technical Specifications
SCADA

Contents

CHAPTER 1: INTRODUCTION & SCOPE of WORK

.

1.0 Introduction

The Nepal Electricity Authority (NEA) has established a Distribution Control Centre (DCC) at the Suichatar Substation premises, which will host the infrastructure for the Distribution Control, System Operations, Network Operations, and associated facilities. This centre currently manages the existing SCADA system covering 30 substations with RTUs within the Kathmandu Valley. To ensure resilience and business continuity, NEA is also planning the establishment of a Disaster Recovery Centre (DRC) in Butwal.

As part of its modernization program, NEA is planning to implement an advanced SCADA system covering 215 distribution substations across its network. The project includes the deployment of new RTUs at all substations, integration with the DCC, 6 regional Grid MCC, LDC, BCC and DRC over a secure Optical Transport Network (OTN) and GPRS (where fiber is not feasible) as backup, and adoption of internationally accepted communication protocols such as IEC 61850, IEC 60870-5 suite, DNP 3.0, and ICCP for inter-control centre communication. This implementation, to be carried out over a three-year duration followed by 4 years of ATS, AMC, and FMS support, aims to significantly enhance operational efficiency, improve reliability, and strengthen supervisory control while ensuring scalability for future network expansions and seamless integration with existing infrastructure.

1.0.1 Proposed SCADA Scope:

The System Integrator (SI), in coordination with NEA, shall be responsible for the survey, design, engineering, supply, installation, testing, and commissioning of a complete SCADA system for the Distribution Control Centre (DCC) and Disaster Recovery Centre (DRC). The project shall be implemented over a period of 3 years, followed by 4 years of Annual Technical Support (ATS), Annual Maintenance Contract (AMC), and Facilities Management Services (FMS). The solution shall include perpetual SCADA software licenses registered in the name of NEA, with no restriction on the number of substations, signals, or data points. The software shall be capable of seamlessly accommodating future expansion, including new substations, without requiring license upgrades or additional costs. The SCADA system will supervise and control all 33/11 kV distribution substations under scope, incorporating Information Storage & Retrieval functions, load shedding applications, and a Dispatcher Training Simulator (DTS).

The hardware infrastructure will comprise servers for SCADA, FEP, ICCP, ISR, historian, DTS, and web applications with load balancing, as well as patch management, antivirus, development, quality assurance, active directory, SMS gateway, and directory servers. External storage, backup systems, workstations, development consoles, DTS consoles, network switches, routers, and comprehensive cybersecurity devices including firewalls, IDS/IPS, VPN, and router-firewall combinations shall be provided. Supporting devices such as GPS-based time synchronization systems, digital time displays, and required peripherals will be included. At the substation level, Remote Terminal Units (RTUs) shall be installed with associated panels, racks, CPUs, converters, wiring, and accessories. Each RTU will be integrated with communication modems, multifunction

transducers, relays, transformer transducers, and Local Data Monitoring Systems (LDMS) with workstation, antivirus, furniture, inverter, and accessories. Test and diagnostic tools including database configuration software, simulators, protocol analyzers, and laptops with interfacing hardware will also be supplied. Auxiliary power systems will be provided at substation level through DC power supply units with VRLA battery backup.

The communication backbone shall be established as a multi-layered, secure, and resilient architecture. The physical underlay will be a high-capacity Optical Transport Network (OTN) using fiber as the primary medium, providing robust, long-haul connectivity between substations and the DCC and DRC-BCC The OTN will serve as the digital "wrapper" that encapsulates all client signals. On top of this secure OTN layer, a Multiprotocol Label Switching - Transport Profile (MPLS-TP) network will be deployed to provide connection-oriented, packet-based transport for all mission-critical data, including SCADA and tele protection in some substations. For backup, secured GPRS will serve as a redundant channel to ensure communication with both the DCC and DRC-BCC. The entire system shall comply with international communication protocols and standards including IEC 61850, IEC 60870-5 suite, DNP 3.0 over TCP/IP, GOOSE messaging, MMS, and ICCP (TASE.2 or higher) for inter-control center communication. Multifunction devices shall interface via Modbus or IEC 61850, while metering systems will conform to DLMS/IEC 62056 with full support for COSEM features.

Cybersecurity shall be embedded across the solution with compliance to ISO/IEC 27001, IEC 62443, and NIST Cybersecurity Framework standards. Measures will include penetration testing, vulnerability assessments, regular patching, encryption, key management, and strict access control policies aligned with NEA's cybersecurity requirements. Testing and validation will be carried out through Factory Acceptance Tests (FAT), Site Acceptance Tests (SAT), and type tests, with clearly defined test cases, performance benchmarks, and point-to-point as well as simulated testing prior to deployment.

Upon successful completion of implementation and acceptance, the SI shall hand over the system to NEA and provide comprehensive ATS, AMC, and FMS support for a period of three years, ensuring continuous operation, maintenance, and compliance with service level agreements.

SCADA System Software Licensing Requirements:

The System Integrator (SI) shall supply the SCADA system software license as a perpetual license registered in the name of NEA. **The System shall be licensed for an initial capacity of at least 150,000 data points, expandable to 250,000 points without software architecture changes**. An indicative sizing of the number of points is provided below for reference. However, the final sizing and point count shall be determined by the SI during the detailed site survey and system design phase.

Sr. No.	For all 33/11 kV Distribution Substations under the scope (215 Nos)	
1	Total DI Signals (CMR)	68370
2	Total DO Signals (HDR)	8170
3	Analog Signals (Without MFT)	1720
4	Analog Signals (with MFT)	51600
	Estimated INITIAL Total signals	129860

During the project duration, if any new substations are added, the SI may claim the contracted BOQ

cost associated with the supply and integration of all SCADA System RTU, Part-B. However, the SCADA system software provided must be capable of seamlessly accommodating additional substations and associated signals/points without requiring any license upgrade or incurring additional costs to NEA due to sizing limitations upto 2,50,000 points.

1.0.2 Broad Role Definition for SI

The System Integrator (SI), in coordination with the Nepal Electricity Authority (NEA), shall be responsible for carrying out the field survey, design, engineering, supply, installation, testing, and commissioning of the SCADA system for 215 Nos. 33/11 kV distribution substations (Quantity of Substations and total signals to be proposed by SI during survey and to be submitted to NEA for approval), the Distribution Control Centre (DCC) at Syuchatar, and the Disaster Recovery Centre (DRC) at Butwal. The implementation will be completed in three years, followed by four years of ATS, AMC, and FMS support. The system shall be designed for future scalability, seamless integration with existing infrastructure, and compliance with internationally accepted standards and protocols.

The key components of the SCADA solutions include & not limited to following:

1) **Software**: The SI shall supply and install all required SCADA software, including SCADA/FEP applications, Historian, ISR, Dispatcher Training Simulator (DTS), LDMS (Local Data Monitoring System), ICCP for inter-control center data exchange, database, virtualization, backup, antivirus, and middleware tools.
    - All software licenses shall be perpetual, registered in NEA's name, and free of limitations on the number of substations, data points, or signals. The software shall be capable of future expansion without additional license cost.
    - The Distribution SCADA system (DCC/DRC) must be sized to manage 215 total Distribution Substations (DSs) estimating the below I/Os, however, the total count of I/Os shall be finalized by the successful bidder post field survey. **The System shall be licensed for an initial capacity of at least 150,000 data points, expandable to 250,000 points without software architecture changes.**
    - The software shall enable integration with external control centers on ICCP (TASE.2 or higher), specifically supporting 6 regional Grid MCCs, LDC, DCC, and DRC/BCC.
    - The application must integrate data from existing SCADA, DMS and OMS applications catering to 30 SS in Kathmandu Valley, existing 18 SS where Distribution SAAS is implemented, upcoming GIS application, Country Wide DMS OMS application, appx 30 FRTUs procured under various projects.
    - The SI shall also deliver operating systems, database, virtualization software, backup, antivirus, and middleware tools required to ensure performance and security including Database, display, and report development.

2) **Hardware:** The SI shall supply, install, and commission all hardware at DCC, DRC, and substations.
    - **Servers**: SCADA, FEP, ICCP, Historian, ISR, DTS, NMS, Patch Management, Antivirus, Development, QA, and Directory servers with redundancy.
    - **Workstations and Consoles**: Substation monitoring consoles, DTS consoles, and development consoles with dual monitors.

- **Network & Security Equipment**: Layer II/III switches, routers, DMZ firewalls with IDS/IPS, VPN, and router-firewall combinations.
- **Storage & Backup**: RAID storage arrays, DAT drives, and external backup devices..
- **Substation-Level Hardware**:
  i. Remote Terminal Units (RTUs) with racks, power supply modules, CPUs, converters, and accessories etc.
  ii. Communication modems (GPRS) and OTN.
  iii. Multifunction Transducers (MFTs), transformer transducers, Contact Multiplying Relays (CMRs), Heavy Duty Relays (HDRs), and dummy breaker latching relays.
  iv. Local Data Monitoring Systems (LDMS) including workstation, antivirus, power backup, furniture, and accessories.
- **Auxiliary Power Systems**: DC power supply systems (DCPS) with VRLA battery banks at all substations.
- **Time Synchronization**: GPS-based time synchronization systems and digital display units.
- **Test Equipment**: Database configuration tools, simulators, protocol analyzers, and laptops with interfacing hardware.

All supplied hardware shall be state-of-the-art, sized for ultimate system expansion, and meet performance, availability, and cybersecurity requirements.

3) **Communication Network:** The SI shall design and deploy a multi-layered, secure communication backbone:
   - **Primary Network**: Optical Transport Network (OTN) for high-capacity fiber-based connectivity between substations, DCC, and DRC.
   - **Redundancy:** Secured GPRS modems at all substations to ensure backup communication.
   - **Protocols:** Compliance with IEC 61850, IEC 60870-5, DNP 3.0, DLMS/IEC 62056 (for metering), and ICCP (TASE.2 or higher).
   - **Integration:** Seamless interfacing with relays, multifunction devices, and IT/legacy SCADA systems shall be ensured using industry-standard protocols such as Modbus, TCP, IEC 60870-5-101/104, IEC 61850 (MMS, GOOSE, Sampled Values), OPC, DNP3, ICCP/TASE.2 or higher, and CIM/XML (IEC 61970/61968), thereby enabling real-time, reliable, and interoperable communication across all systems.
4) **System Design:** The System Integrator (SI) shall be responsible for preparing comprehensive Functional Design Specification (FDS) documents for both hardware and software, based on detailed site surveys and requirements gathered from NEA.

   The design scope shall include, but not be limited to:

   a) **Integration Scope:** The architecture design must explicitly cover SCADA system topology, communication links, middleware, and integration with RTUs, FRTUs, 18 SAAS, 6 Grid MCCs, LDC, DCC, and DRC, future applications for a complete, integrated network view.
   b) SI should prepare and propose Hardware Sizing & Layouts: Server and storage sizing, redundancy configuration, workstation requirements, networking equipment, and layout of racks, consoles, and field devices.
   c) Database & Application Design: Design of SCADA database, historian, and application layer including HMI/GUI displays, reports, and alarms, with expandability for future

growth.

d) Electrical & Civil Works: Cabling, earthing, grounding, power backup systems, layouts.

SI should submit all Design & Drawing documents, Quality Assurance plan (QAP), Tesh schedule & plans, reports, and operation/maintenance manuals for NEA's review, comments, and approval.

5) Facilities management services (FMS): The SI shall provide Facilities Management Services (FMS) (after successful completion) for operation and maintenance of the SCADA system and associated infrastructure supplied and commissioned under this project. The scope shall include:

a) **Database & System Updates:** Creation, modification, addition, and deletion of databases, RTU configurations, displays, reports, and limit settings in line with changes and growth in NEA's electrical distribution network.

b) **Service Duration:** The FMS shall be provided for a minimum of four (4) years after successful completion of Operational Acceptance Tests (SAT) of the SCADA System.

c) **System Management:** The Contractor shall manage the entire system—including hardware, software, networks, and installations—ensuring that they meet the specified availability and performance requirements.

d) Coordination & Single Point of Contact:

- The Contractor/SI will act as the Single Point of Contact (SPOC) for all Service Level related issues.
- Coordination with other Service Providers/vendors shall be carried out as required.
- During the warranty period, the prime responsibility of service delivery rests with the Lead Contractor (System Integrator).
- Post warranty, the Contractor shall continue coordination with other vendors as selected by NEA.

e) Maintenance & Security:

- Provision of both software and hardware maintenance support for the SCADA system and communication network.
- Execution of interim system audits in case of major changes.

f) **Warranty Supervision:** The Contractor shall supervise and operationalize the four-year warranty of the SCADA system and communication network following Operational Acceptance.

The role of the Contractor as FMS provider shall commence immediately after installation, commissioning, and Operational Acceptance / SAT of the SCADA system.

6) Supply of Equipment and Material: The System Integrator (SI) shall be responsible for the manufacture, inspection at manufacturer's works, supply, transportation, insurance, delivery at site, unloading, storage, supervision, installation, and successful commissioning of all equipment, systems, and application software under the project. All proposed deliverables shall be of state-of-the-art design and conform to best practices in architecture and engineering, the During execution , warranty is SI responsibility. Moreover, SI shall provide a minimum 4 (four) year warranty along with a comprehensive support plan from the respective OEMs to align with the Facility Management Services (FMS) timeline.

Furthermore, any item, though not explicitly mentioned in the specifications but essential for the safe, reliable, efficient, and trouble-free operation of the system and to meet the performance, availability, and functional requirements defined in the RFP, shall be deemed included in the Contractor's scope. Such items shall be supplied, installed, and commissioned by the SI without any additional cost to NEA.

7) Testing and Acceptance:

The System Integrator (SI) shall be responsible for conducting all testing and validation processes required for the successful implementation, integration, and acceptance of the SCADA system, in compliance with NEA specifications. Testing shall include, but not be limited to, the following stages:

a) Type Testing:

- All equipment offered shall comply with type tests as per relevant standards and technical specifications.
- Valid test certificates (from accredited labs, within five years or as specified) shall be submitted for review.
- In case of non-compliance or absence of valid certificates, fresh type testing shall be carried out by the SI at no additional cost to NEA.

b) Ad-hoc / Prototype Testing (Optional):

- SI shall demonstrate prototype SCADA functionality with at least four RTUs and balance points simulated, as required by NEA.
- Such tests may be conducted during the design and engineering stage for early validation.

c) Factory Acceptance Test (FAT):

- Conducted at the SI/manufacturer's premises for hardware, software, and equipment prior to dispatch.
- Shall cover hardware integration, functional performance, interoperability, cybersecurity compliance, and continuous operation tests.
- FAT test procedures, test cases, and test data shall be prepared by SI and approved by NEA.
- All required logistics for NEA officials (including airfare, visa facilitation, transportation, boarding, and lodging) shall be arranged and borne by the SI to facilitate factory inspections.
- Submission of detailed FAT reports and clearance from NEA is mandatory before shipment.

d) Site Acceptance Test (SAT):

- Conducted at project sites after installation and integration of systems.
- Includes field installation tests, end-to-end tests, field performance tests, and deferred FAT tests requiring site environment.
- Validation of complete functionality, data exchange, communication interfaces, cybersecurity compliance, and real-time performance under actual operating conditions.
- Successful SAT shall be the basis for provisional acceptance.

e) System Availability Test (SAVT for 360 Hours):

- Conducted after SAT to demonstrate 99% system availability (hardware and software) over 360 hours (15 days), with no outage in the final 85 hours.
- Includes testing of redundancy, failover, real-time operations, and integration with RTUs, substations, and external systems.
- Any shortfall in availability shall be corrected and re-tested by SI at no additional cost to NEA.

f) Cybersecurity Compliance Testing:

- Verification of compliance with ISO/IEC 27001, IEC 62443, and NIST Cybersecurity Framework.
- Includes penetration testing, vulnerability assessments, encryption validation, and audit by NEA/authorized security agency before operational acceptance.

g) User Acceptance Test (UAT):

- To be conducted at NEA's Distribution Control Centre (DCC) after 100% completion of SCADA scope and under the supervision of NEA Project Manager.
- Validates operational workflows, databases, displays, reports, alarms, and user-defined functions against NEA's operational requirements.
- Successful completion of UAT is a prerequisite for final handover and operational acceptance.

h) Documentation:

- SI shall prepare and submit detailed, test plans, test specifications, test cases, test data, and test reports for each stage.
- All documents (FDS-Functional Design Specifications, HDS-hardware design specifications, test procedures, reports, cybersecurity plan, interoperability profiles, "as-built" drawings, etc.) shall be submitted in both hard copy and electronic form for NEA's review and approval.
- The SI shall ensure that any deficiencies observed during FAT, SAT, SAVT, or UAT are promptly rectified without any additional cost implication to NEA.

8) Annual Maintenance Contract (AMC) and Annual Technical Support (ATS)

To ensure sustained and reliable operation of the SCADA system and associated communication infrastructure, the Contractor/SI shall provide comprehensive AMC and ATS services post operational acceptance.

a) Annual Maintenance Contract (AMC): The AMC shall cover hardware, field equipment, and auxiliary systems supplied and commissioned under the project. The scope shall include:

- Preventive and corrective maintenance of SCADA and communication hardware.
- Supervision of warranty obligations of OEMs and third-party suppliers.
- Availability of spares, timely replacement of defective modules, and restoration of faulty equipment.
- AMC for auxiliary systems including UPS, power supply equipment.
- O&M of ADSS cable and associated optical network infrastructure, including inspection, splicing, and emergency restoration.

b) Annual Technical Support (ATS): The ATS shall cover software, applications, and databases to maintain system availability and performance. The scope shall include:

- OEM-backed updates, patches, and software version upgrades.
- 24x7 technical helpdesk and remote troubleshooting support.
- Assistance in database modifications, report generation, and new RTU integration during the ATS period.
- Cybersecurity updates, vulnerability management, and compliance with NEA's security framework.
- Escalation to Level 3 support with OEMs for critical issues.

The Contractor shall act as the **Single Point of Contact (SPOC)** for all AMC/ATS issues, coordinating with vendors and OEMs as necessary to meet the agreed Service Level Agreements (SLAs). AMC and ATS shall remain in force for 4 (four) years post-SAT, aligned with the Facility Management Services (FMS) period.

9) **Integration Scope: SI** should ensure that legacy systems (SAAS, Existing SCADA, LDC, BCC etc) and the new solutions lined up by them are tightly integrated and do not remain stand-alone and shall perform on real time basis as envisaged in specifications. All required external systems shall be integrated using an integration middleware layer. The scope of integration of external systems includes, legacy SCADA system, RTU, IT systems, Numerical relays etc. already existing and functional in the NEA, but outside the present scope of work and defined in RFP by NEA. The integration is expected to be Industry Standards Based on IEC 61968-1 Bus (SOA Enabled on enterprise Bus) using CIM/XML, OPC, ICCP etc., which is, on-line, real time or offline where appropriate and shall operate in an automated fashion without manual intervention, which is documented for future maintenance.

SI shall make necessary provisions/software linkages in the proposed solution so that the IT system or any legacy SCADA system as specified in the RFP may be integrated seamlessly.

10) Cybersecurity shall be embedded across all layers of the SCADA, communication, IT, and integration infrastructure to ensure resilience, data confidentiality, integrity, and availability in line with NEA's cybersecurity policy and international standards. The System Integrator (SI) shall be responsible for implementing, testing, and maintaining end-to-end cybersecurity measures throughout the project lifecycle and during the FMS/AMC period.

The broad scope of cybersecurity compliance shall include but not be limited to the following:

a) Standards & Framework Compliance

- Ensure full compliance with ISO/IEC 27001 (Information Security Management System), IEC 62443 (Industrial Control System Security), and NIST Cybersecurity Framework.
- Map cybersecurity controls to NEA's internal policies and regulatory requirements.
- Document compliance matrix linking implemented security controls with relevant clauses of the above standards.

b) Secure Architecture & Design

- Incorporate defense-in-depth architecture with segregated zones and conduits for IT, OT, SCADA, and corporate systems.
- Ensure use of firewalls, DMZs, intrusion detection/prevention systems (IDS/IPS), and secure VPNs for remote access.

- Enforce end-to-end encryption (AES-256 or equivalent) for data-in-transit and secure key management mechanisms.

c) Identity, Access & Authentication Controls

- Implement role-based access control (RBAC) with least privilege enforcement.
- Enforce multi-factor authentication (MFA) for operator, administrative, and remote maintenance logins.
- Maintain audit trails and system logs for all access attempts, configuration changes, and command executions.

d) Vulnerability & Patch Management

- Perform periodic vulnerability assessment and penetration testing (VAPT) for SCADA, RTUs, servers, and integrated IT/OT assets.
- Implement a Patch Management System with structured patch and update policy, ensuring timely deployment of OS, firmware, and application patches without system downtime.
- Maintain a threat intelligence feed integration to anticipate and mitigate emerging cyber threats.

e) Endpoint Protection

- Deploy endpoint detection and response (EDR) tools, and whitelisting for critical SCADA servers and operator consoles.
- Ensure USB/media control policies to prevent unauthorized data injection.

f) Cybersecurity Testing & Validation

- Conduct Factory Acceptance Test (FAT), Site Acceptance Test (SAT), and type tests with cybersecurity-specific scenarios.
- Define test cases, performance benchmarks, and simulated attack vectors for validating resilience under real-world threat conditions.
- Perform point-to-point security validation of communication links (e.g., ICCP, OPC, GPRS/OTN, MPLS-TP) prior to deployment.

g) Monitoring, Incident Response & Recovery

- Establish SISLOG or equivalent monitoring platform for continuous log collection, correlation, and alerting.
- Define and implement a Cybersecurity Incident Response Plan (CIRP), including detection, containment, eradication, and recovery measures.

h) Audit, Reporting & Compliance Assurance

- Conduct third party in Cyber Security drills (one post FAT & one post SAT) of entire SCADA system.
- Facilitate third-party cybersecurity audits as mandated by NEA.
- Provide quarterly security compliance reports, including incident logs, vulnerability scan reports, and patch status.
- Ensure documentation of configurations, policies, and test results for future reference and certification renewals.

i) Capacity Building & Training

- Provide cybersecurity awareness and technical training to NEA operators, administrators, and engineers.
- Share best practices for secure operations, password hygiene, and incident reporting.

11) Training for Employees:

The System Integrator (SI) shall be responsible for organizing comprehensive training programs for both the core NEA implementation team and end-users to ensure smooth adoption and effective operation of the SCADA solution.

The training program shall be developed in close coordination with NEA's project team to ensure that the training materials, and delivery methods are aligned with the scope. The SI shall prepare all necessary training materials, standards, manuals, and course documentation covering SCADA system architecture, day-to-day operation and maintenance, cybersecurity compliance, database and network administration, troubleshooting, and disaster recovery procedures.

Training shall be delivered in multiple tiers, including core team "train-the-trainer" sessions, end-user training for operators and engineers, and specialized sessions for system administrators on hardware, software, and network security management. Cybersecurity training aligned with ISO/IEC 27001, IEC 62443, and NIST CSF shall also be provided to build awareness and compliance.

The SI shall conduct training both in Nepal and, where required, at the OEM's factory or training centers abroad. For overseas training, the SI shall arrange and bear the cost of airfare, lodging, meals, visa assistance, insurance, and local transportation for the nominated NEA officials. Upon completion of training, participants shall be awarded certificates of successful completion, and the SI shall also conduct pre- and post-training assessments to evaluate effectiveness and provide retraining if necessary.

12) Assist NEA for responding to queries to Nodal Agency: SI will be responsible for preparing responses to the queries raised by the Nodal Agency. Adequate support will be provided by the NEA to the SI.

13) Progress Update: The SI may also provide monthly project reports highlighting critical issues to the NEA. Further, any information progress report, etc. as and when sought by the NEA/ADB/Ministry shall be furnished by the SI.

14) In addition to the above, following works are also in the scope of the contractor:

a. Database, Reports and display development
b. Training
c. Obtaining the statutory clearances required, if any Gov Bodies.
d. All the charges deposited to aforesaid authority for obtaining statutory clearance borne by SI/Contractor, NEA may also provide the necessary support if required in getting the clearances and interdepartmental coordination.
e. Sufficient SPARES /INVENTORY for AMC/ATS period of four years to meet SLA

15) Other Services and Items: The scope also includes, but not limited to the following services/items described herein and elsewhere in specification:

a. **Project Management and Site Supervision:** The bidder/SI shall be responsible for the overall management and supervision of works, including the implementation of risk management as well as change management initiatives. He shall provide

experienced, skilled, knowledgeable and competent personnel for all phases of the project, so as to provide the NEA with a high-quality system.

b. **Interface Coordination:** The bidder shall identify all interface issues with NEA and other agencies if any, and inform NEA in writing which shall interface, coordinate and exchange of all necessary information among all concerned agencies.

c. **Scope Change Management:** NEA to finalize the scope change management procedure during development/Implementation stage

d. Dedicated earthing and surge protection shall be provided for SCADA equipment, including RTUs, to protect against fault currents and voltage surges, in compliance with relevant IEC standards.

16) The responsibility of the Contractor shall include supplying, laying and termination of the cables, wherever required for:

(a) Acquiring analog data using MFT, transducer, sensor which shall be connected with the primary devices.
(b) Acquiring the digital data for status of field devices relays in the control room.
(c) Extending control output to field devices through heavy duty relays.
(d) Interconnection between Contact Multiplying Relays (CMRs) and RTUs, field devices (CMRs to be supplied by the contractor as per BOQ),
(e) Power and signal cabling between the supplied equipment & Owner's equipment Incl. outdoor panels
(f) Any other cabling required for completion of the project.

1.0.3 Specific Exclusions

The SI is not expected to address the following:

(a) All internal and external electrification, Air conditioning and ventilation, fire-fighting system and Access control system required for SCADA system are outside the scope of the SI, however contractor has to indicate the space requirement for DCC, BCC, RTU /Auxiliary power supply & communication equipment any other specific requirement, power supply requirement including standby supply requirement, so that the NEA can provide the same as per bidder's requirement
(b) Note: While major civil works (building construction) are excluded, the System Integrator (SI) IS RESPONSIBLE for minor civil works required for equipment installation, including grouting of panels, wall drilling/sealing for cable entry, and supply/installation of cable trays/trenches within the control room/substation building
(c) Manpower required operating SCADA system.
(d) A.C. input power supply

1.0.4 Generic requirements (SCADA)

The contractor shall undertake detailed site survey immediately after award of the contract of all the sites to access the various requirements such as space, identification of input terminals, and availability of spare contacts etc. for completion of engineering, site installation, testing and commissioning of the project. The type and number of hardware and software elements (Bill of Quantity) within the scope of the project to be supplied for the various sites are identified. The individual functions to be performed by the hardware and software and system sizing criteria are described in the relevant sections. The specification defines requirements on functional basis and does not intend to dictate a specific design. On the other hand, certain minimum requirements must

be met in accordance with the particular details provided elsewhere in the specification.

The items, which are not specifically identified but are required for completion of the project within the intent of the specification, shall also be supplied & installed without any additional cost implication to NEA.

1.0.5 Requirements Gathering and Solution Design

The Bidder's proposal shall address all functional, availability and performance requirements within this specification and shall include sufficient information and supporting documentation to determine compliance with this specification without further necessity for enquiries.

An analysis of the functional, availability 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 added cost to NEA all such additional items and services such that a viable and fully functional system is implemented that meets or exceeds the capacity, and performance requirements specified. Such materials and services shall be within the scope of the contract. To the extent possible, the Bidders shall identify and include all such additional items and services in their proposal.

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 offered items shall be designed to operate in varying environments including suitability as per higher altitude requirement. Adequate measures shall be taken to provide protection against rodents, contaminants, pollutants, water & moisture, lightning & short circuit, vibration and electro-magnetic interference etc.

The Contractor shall demonstrate a specified level of performance of the offered items during well-structured factory and field tests. Further, since at the substations limited space is available the contractor shall make all the efforts to economize the space requirement.

The Bidders are advised to visit sites (at their own expense), prior to the submission of the proposal, and make surveys and assessments as deemed necessary for proposal submission. The successful bidder (Contractor) is required to visit all sites. The site visits after contract award shall include all necessary surveys to allow the contractor to perform the design and implementation functions.

After the site/route survey the Contractor shall submit a survey report for all the sites. This report shall include at least the following items; however, the exact format of the report shall be finalized by the contractor with the approval of NEA.

a. Detailed requirement gathering exercise for roll out of SCADA System.
b. Overall sizing and designing of SCADA system should be based on the As-Is status study
c. Submit a detailed solution and deployment architecture of the SCADA system. (HLD & LLD Reports)
d. The finalized proposed solution architecture should be submitted and approved by the NEA before solution customization, development and roll out.
e. Assessment of the end user capacity level at each location and suitably modify capacity building/change management programs in consultation with the NEA.

f. Proposed layout of Equipment in the existing rooms and buildings.

g. Proposed routing of power, earthing, signal cables and etc.

h. Confirmation of adequacy of Space and AC Power supply requirements

i. Proposals for new rooms/buildings, if required

j. Identification of facility modifications, if required

k. Identify all additional items required for interconnection with the existing equipment.

l. Requirement of Modification to existing earthing arrangement, if any.

1.0.6 Facilities to be provided by NEA

a. Arranging necessary shutdowns and work permits at various sites.

b. Formation of team for SCADA works at substations and field level (if required) both.

c. Timely approval of documents, tests etc.to ensures completion of project in time.

d. Timely release of payment to contractor on achievement of milestones/compliances

e. Retro fitment of breaker for SCADA ready

f. Providing storage space at site free of cost wherever available. Special storage needs such as watch and ward services and air conditioning shall be provided by the contractor.

h. The existing earthing system at the substations may be utilized for earthing of the offered equipment. However, it is essential that the contractor shall assess its suitability for the offered equipment and carry out the modifications if required. It is recommended to provide separate electronic earthing for SCADA equipment's by contractor.

i. Suitable space/Infrastructure incl. civil works, electrical raw supply, Air-conditioning, firefighting, building security, lighting, furniture etc. for Control center/DR, Substations for installation of control center/ DR equipment's, RTUs etc.in line with SCADA system implementation schedule.

j. Providing details of Existing Legacy systems if any SCADA, RTU, IT, Numerical relays etc.

k. NEA shall ensure that Project implementation & operation to be done by O&M dept. of NEA where IT dept. /cadre shall work as support. This is mandatory

1.0.7 Items of Special Interest for SCADA

The database displays and reports for SCADA system are to be developed by the contractor; however, the contractor shall associate NEA engineers also during the data base development. The required hardware & software for completion of this activity may be used out of the hardware & software to be supplied under this contract. Integration with NEA's Existing SCADA, LDC, MCC & BCC.

1.0.8 Warranty (SCADA Solution)

This would include five years warranty for the related hardware & software supplied under the SCADA project after the Site acceptance test (S.A.T), operational acceptance of the SCADA System. The five-year warranty shall include comprehensive OEM on-site warranty for all components (H/W and Software including OS) supplied including reloading and reconfiguration of all Software and device drivers/patches etc. if required. In case five Years warranty is beyond standard warranty period of the equipment or required to cover to cover FMS

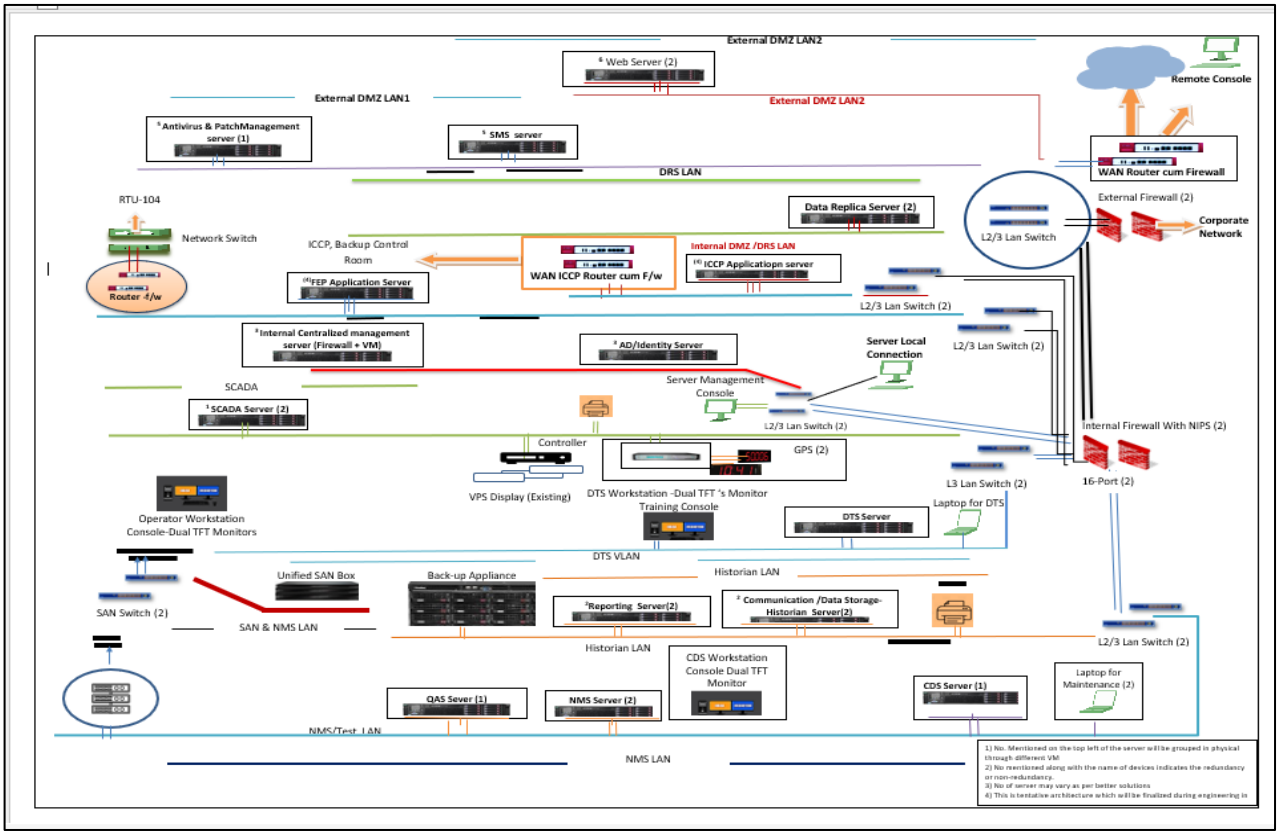
period, the extended warranty shall be the responsibility of SI.

1.0.9 Terms for NEA & SI

The term contractor & bidder shall be referred as System Integrator (SI) & owner; employer shall be referred as NEA wherever mentioned in the RFP.

1.0.10 Proposed SCADA system

The diagram below illustrates the SCADA system architecture, highlighting the key components. However, the final architecture must be designed and submitted by the Contractor / SI during the design phase and approved by NEA for implementation.



1.0.11 Integration Requirements with Existing SCADA

SCADA integration with legacy system SCADA to ensure seamless interoperability, centralized monitoring, and unified control across both existing and newly integrated substations.

The bidder shall conduct a detailed survey to assess the existing legacy system architecture and shall be responsible for implementing necessary protocol converters or gateways, mapping data points, ensuring time synchronization, configuring communication interfaces, and performing end-to-end interoperability testing to enable seamless integration with the new SCADA system.

1.0.11.1 Integration with existing SCADA System for NEA Substations

The SCADA Expansion Project shall involve the integration of 30 existing SCADA-enabled substations located both within and outside the Kathmandu Valley, including remote areas. The objective is to establish a unified and centralized SCADA system for comprehensive monitoring and

control across the NEA substation network. The scope includes seamless interfacing with existing field devices such as Remote Terminal Units (RTUs), Feeder RTUs (FRTUs), Intelligent Electronic Devices (IEDs), and Advanced Metering Infrastructure (AMI).

Each substation shall be equipped with fully functional RTUs and IEDs capable of reliable, secure, and real-time communication with the SCADA master station and backup control centers. All RTUs must support standard protocols such as IEC 60870-5-104, IEC 61850, or DNP3 to ensure interoperability across multi-vendor environments.

Substations located outside the valley shall utilize secure and robust communication links, including fiber optic/MPLS/VSAT, depending on site-specific conditions. The system shall incorporate redundant communication paths and automatic failover mechanisms to ensure high availability and uninterrupted connectivity with the SCADA control centers. This integration will enable centralized data analytics, enhance situational awareness, and support efficient, data-driven decision-making through a unified dashboard interface.

1.0.11.2 Integration with existing SCADA System at LDC, MCC & BCC.

The S.I shall ensure seamless, secure and real-time data exchange between new and existing SCADA system for monitoring, Control, redundancy or backup operations on IEC 60870-6 TASE.2 (ICCP protocol with latest version) at the Load Dispatch Centre (LDC), MCC & BCC with applicable cyber security standards and guidelines.

The S.I shall also ensure compatibility with the data communication architecture and operational protocols currently deployed at the LDC.

1.0.12 System Go-Live and Acceptance Criteria

The purpose of this section is to collate the information regarding the state of the project prior to declaration and acceptance of the Go - Live. Whilst there are certain mandatory criteria for declaring the Go-Live however they might be exempted & relaxed, in case of any exception and appropriate approval from the NEA authority.

These include the following document requirements:

- Submission of Project Documentation and Deliverables and requisite sign offs obtained.
- Hardware and software for SCADA and RTUs have been tested, supplied, installed, and commissioned for both DCC and BCC as per the scope.
- Network connectivity provisioned and communicating at all locations as per scope.
- Completion of Software customizations.
- User Acceptance Testing Completed.
- Functional Requirement specifications (FRS) compliance achieved.
- Fit/Gap Analysis Completed.
- Ensure that all SLA requirements are met prior to the Go-Live declaration
- Training provided as per schedule and scope approved by NEA
- Software Change and Release Management Process in Place as per NEA acceptance
- Exit Management and Handover Plan Accepted by the NEA

- Detailed Schedule Available for Go - Live
- Roll Back Plan Available
- Adequate FMS, ATS and AMC plan in place for Handover
- Scope of Work Completed and Signed off by NEA.

----- **End of Chapter 1** -----

CHAPTER -2: SCADA FUNCTIONS

2.0 General requirements

This chapter describes the functions to be performed by the SCADA applications for NEA. Bidders are encouraged to supply standard, proven & tested products that meet or exceed the specification requirements. This chapter describes the requirements of ISR functions also. Unless specified as optional functions/ features all functions/ features mandatory for the project.

2.1 Design requirements

The software shall be modular in nature. The software shall be able to work platform based on minimum 64-bit architecture. All the variable parameters of SCADA applications, which require adjustment from time-to-time, shall be defined in the database and shall be adjustable by system personnel. 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 user or programmer shall become effective without having to reassemble or recompile programs or regenerate all or portions of the database.

The specific requirements for output results are described along with the other requirements of each function. However, all results that the user deems to be important shall be stored in a form accessible for display and printing.

2.1.1 SCADA Function Access

Various application functions shall be designated as single user/ multi-user. For a single-user function, the user with access to the function must relinquish access to it before access can be granted to another user. For a multi-user function any number of users, up to the maximum designated for the function, may have access to the function simultaneously. All such actions shall be recorded as events in the event log.

2.1.2 Critical & noncritical functions

The functions defined in this specification shall be classified as Critical or as non-critical. Every critical function must be supported by sufficient hardware & software redundancy to ensure that no single hardware & /software failure will interrupt the availability of the functions for a period exceeding the automatic transfer time defined in the specification.

Non-critical function may not be supported by hardware & software redundancy and can be suspended in case of non-availability of corresponding hardware.

Generally, the following are to be classified as Critical functions: -

a) All SCADA applications
b) Information Storage and Retrieval (ISR)
c) Load Shed application (LSA)
d) Outage data analytics and reporting (ODAR)
f) Data exchange among the contractor supplied SCADA & IT system established
g) Web server applications, Security applications

h) Network Management system (NMS)

i) Disaster Recovery & Data recovery function (DR) / Backup Control Center function

The following are non-Critical functions

a) Dispatcher Training Simulator (DTS)

b) Database modification and generation

c) Display modification and generation

d) Report modification and creation

e) Data exchange with Remote VDUs, if any

2.2 SCADA Functions

The following SCADA functions are envisaged under this specification.

- Data Acquisition from RTUs at Substations
- Time synchronization of RTUs
- Continuous real-time data storage and playback
- Sequence of event processing
- Supervisory Control for all substations
- Fail-soft capability
- Remote database downloading, diagnostics & configuration
- CIM compliance IEC61968
- Information Storage & Retrieval (ISR)
- Load Shed Application (LSA)
- Data recovery function (DR) or Backup control center (BCC)

The SCADA system shall have capability to accept data from the following sources:

a. Telemetered data received from RTUs

b. Calculated data

c. Pseudo-data (Manually entered data)

All input data and parameters, whether collected automatically or entered by a user, shall be checked for reasonability and rejected if they are unreasonable. 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 in the presence of unreasonable data.

Each of the SCADA functions is described below.

2.2.1 Communication protocol.

SCADA system shall use the following protocols to communicate

a) IEC 60870-5-104/101 for RTUs to control centers.
b) MODBUS or IEC 60870-5-101/104 – MFTs to RTUs
c) ICCP (TASE.2 or above) between SCADA Control centers etc.
d) Support /compliance to IEC61850, IEC60870-5 suite for RTU/CC
e) Support/compliance to IEC 61850 for substation automation, including GOOSE messaging, MMS protocols.
f) Support /compliance to DLMS/ IEC 6205.
g) Specify compliance levels for DLMS/COSEM, including profile management, firmware upgrades, and time synchronization.
h) Adherence to cybersecurity compliance in accordance with international standards such as ISO/IEC 27001, NIST Cybersecurity Framework (CSF), and IEC 62443. This includes conducting penetration testing, vulnerability assessments, and implementing periodic updates to address emerging threats.

The protocol considerations shall be made in accordance the system/ device to be interfaced. However, system shall have capability to interface using all necessary protocols as specified above for the devices that may be interfaced in future.

2.2.2 Data Acquisition

SCADA system shall acquire data from Remote Terminal Units (RTUs), MFTs. The type of data to be acquired through RTUs, MFTs shall include analog values, digital status data (Double point and single point indications) and SOE data from the substations etc.

Analog values like P, Q, F, each phase V, each phase I, each phase pf, and energy values (Export/Import KWh and KVARh) shall be collected by the RTU from the MFTs. Analog values such as station battery voltage, oil temperature, winding temperature, tap changer transducer data etc. shall also be acquired through RTU using analog input modules & suitable transducer, if defined in the RTU BOQ.

2.2.2.1 Polling method

Digital status data from RTU shall be reported by exception and shall be updated and displayed within 3 seconds. Digital status data shall have higher priority than the Analog data. The system shall have dead band for data by exception.

All analog values except energy values shall be reported by exception from the RTU. The analog value, when reported by exception, shall be updated & displayed within 4 sec from S/S. An integrity scan of all status & Analog values shall also be made every 10 minutes (configurable).

The provision shall also be made to report analog values & status data periodically at every 10sec (user configurable), if required by the user.

Energy values of 15-minute blocks shall be collected periodically from the RTU at scan rate of 15 minute/1 hour (configurable up to 24 hours). Alternatively, the energy values shall be calculated for each 15 minutes/1 hour blocks at SCADA level from the acquired energy values of MFTs through RTU.

The contractor must assess & take the network delay into consideration while designing the system so that the update time in normal & peak level of activities are met.

The SCADA computer system shall also be able to collect any and all analog & digital data from its RTUs on demand. Apart from the periodic integrity scan, the integrity scan shall also be initiated automatically for an RTU whenever the following situations arise:

i. Upon startup of the system
ii. On demand by SCADA functions
iii. On request by the user

The TCP/IP Communication for RTU on public network shall be encrypted over SSL Security / VPN & the equipment should take control command from designated Master IP address only and no other IP. The RTUs & all TCP/IP devices that are on Public Network shall form a private VPN network with the SCADA Front End, through which encrypted data gets exchanged.

2.2.2.2 Telemetry Failure

If data is not received from an RTU/ after a user-adjustable number of retries, each affected point in the SCADA system shall be marked with a **'telemetry failure quality code' and** an alarm shall be generated. Telemetry failure of data can be due to failure of communication, failure of complete RTU module or MFT etc. Only a single alarm shall be generated if an entire RTU or its communication channel fails.

In the event of telemetry failure, the last good value/status shall be retained in the database for each affected point. When telemetry returns to normal, the associated SCADA system shall automatically resume updating the database with the scanned data.

The user shall be able to substitute a value in the database for any point that is experiencing telemetry failure which shall be marked with **'manual replaced' quality code** in addition to the **'telemetry failure' quality code.** The user shall also be able to delete any point (or entire RTU) from scan processing. All deleted points shall be marked with a **'delete-from- scan' quality code.**

Acquisition Modes

The following modes of data acquisition shall be supported:

a. Enable: When RTU is enabled, the data is scanned in normal fashion and control command execution is allowed.
b. Disable: When RTU is disabled, the data scanning & control execution is disabled. This is equivalent to" delete from scan "of complete RTU
c. Test /Maintenance

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 shall be marked in the database with a quality code 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 of points that are in the test mode shall not be permitted.

When an RTU is removed from the test mode, a message shall be generated, the test mode quality code shall be removed from all points assigned to the RTU, the database values hall resume updating on each scan, and any controls for the RTU shall be enabled.

2.2.3 Time synchronization of RTUs

The SCADA system will be synchronized from the GPS based Time and frequency system. The SCADA system shall synchronize the time of all connected RTUs every 15 minutes (user configurable from 5 minutes to 24 hrs.) using time synchronization message in the IEC 60870-5-104/101 protocol /NTP/SNTP. The servers /Workstations at SCADA control center shall be synchronized using NTP/SNTP. The time of DR center (backup control center) shall also be synchronized from the GPS based system installed in one of the associated SCADA control center or SCADA centre.

2.2.4 Data exchange between SCADA control centers (DCC) & BCC center:

If opted & requirement specified by NEA, then SCADA control centers shall also exchange data using ICCP with Load Dispatch Centre (LDC) of the state. Data exchange shall also allow other information to be transferred report by exception but also configurable periodically, or on demand. It shall be possible to exchange at least the following data:

a. Real-time telemetered data of the interconnected network,

b. Non-telemetered data of the interconnected network,

c. Calculated data of the interconnected network,

d. SOE data of the interconnected network

e. Historical data of the interconnected network

f. Scheduling data

g. Operator messages.

h. Event /alarm lists

Disaster recovery is replica of main control center and hence shall be in sync on daily basis or on demand also.

The data exchange with backup control center (BCC) is required all the data to be transferred from SCADA control center (DCC) which is required for system build. ICCP (TASE.2 or above) protocol or equivalent nonproprietary/ De-Facto protocol shall be used transfer network model / database changes on incremental /global basis automatically once a day & on demand. It shall transfer all data /information which are required for system build.

2.2.5 Data Processing

The SCADA system shall prepare all data that they acquire for use by the power system operations and other applications. The data processing requirements shall apply to data collected from all specified sources.

Data acquired from RTUs/IT system, as well as data received from the existing control centers (if any and specified by NEA in this RFP), shall be processed and placed in the Real-Time Database as soon as it is received.

Data processing involves a value which has been converted to internal form and analyzed for violations of limits. The data processing shall set various data attributes depending on the results of the checks and shall trigger any additional processing or calculation. 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 /IT system / backup control center and RTUs etc.

b. Calculated data

c. Manually entered data

d. Sequence of events data

e. Alternate data sources

2.2.5.1 Analog Data Processing

Analog data processing shall be performed according to the requirements listed below.

(i) Conversion to Engineering Units

Analog points that are transmitted to SCADA system in raw data format shall be converted to engineering units before being stored in the database. This conversion function shall include, as a minimum, the capability to perform the following conversion algorithm:

Value = (A * scanned valued) + B,

Where A and B are programmer-adjustable constants assignable as database attributes on a per point basis.

(ii) Zero dead band processing

The SCADA system at control center shall process each analog input for dead band zone processing. The acquired value, if falls between the dead band range around zero then it shall be considered as clamped zero value else the actual value shall be considered.

(iii) 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 a return-to-normal message shall be generated.

(iv) 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. Generally, any alarm can be assigned as audible alarm but emergency limit shall necessarily be assigned as audible alarm.

All telemetered 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. Whenever a monitored point crosses a limit in the desirable direction, an exit alarm message shall be generated. If multiple

limits have been crossed since the last check, each limit crossed shall be reported.

All limit monitoring shall preclude annunciation of multiple alarms when a value oscillates about an alarm limit by utilizing a programmer-adjustable alarm dead- band for each point. The user shall be able to temporarily override any of the above limits (which are in use) by entering a new value. When the user overrides a limit, it shall be marked with a **'limit override quality code'** on all displays. The override value shall be recognized, and any display, report, or log containing 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 or system is re- initialized. Any change in alarm states resulting from a change in limit value shall be reported. Contractor shall finalize & take approval from NEA for limit values.

(v) Rate of change /Gradient

All telemetered and calculated analog points shall also be processed for rate of change / Gradient processing, if defined that point for such processing in the database. An Alarm for overshoot & event message for return to normal shall be generated.

The rate of change shall be calculated periodically for each assigned point, by dividing the point's values at the beginning and the end of the period into the length of the period. Filtering shall be applied so that single scan excursions do not cause an alarm. The result shall be saved as a non-telemetered database point. All the requirements that apply to calculated points, such as limit checking,

Alarming and availability for display and processing shall apply to the ROC points. There shall be a positive limit and a negative limit to catch excessive rises in the analog value.

(vi) Sign Conventions

The sign conventions for the display, data entry and reporting of active and reactive power flow shall be used universally by all SCADA functions. All imports to bus bars shall be represented with + sign and all exports from bus bars shall be with –ve sign.

(vii) Accumulator Processing

The system shall be able to store accumulator history. Storing accumulator history shall be provided with a method in which that stores data only once per hour and in other method that stores data each time new data enters the system.

It shall be possible to use the two methods concurrently for any pulse accumulator, making it possible to maintain two records for data that are read more than once an hour.

2.2.5.2 Digital Input Data processing

Each state of a digital input point shall be associated with the state of an actual device. The number of bits that will be used to define the state of a device is defined in the RTU Specification. A status point shall be defined as being either legal or illegal, and normal or abnormal:

a. **Illegal state:** The first check on a new input to a digital status point is the legality check. If the new state is illegal, then the old value shall be left in the database and marked old with relevant quality code such as telemetry failure etc.

b. **Abnormal state:** If the new state is legal, it shall be checked to see if it is among the normal states defined for the point. If not, the status point shall be marked as abnormal.

While abnormal, it shall appear in the summary display of abnormal conditions/ off-normal summary

c. **Alarm checking:** Each new value shall be checked to see if transitions into that state are to be alarmed. If so, and if no control action is pending on the status point, then an alarm action shall be triggered.

The following digital input data types shall be accommodated as a minimum:

a. Two-state points: The following pairs of state names shall be provided as minimum:
   1. Open/Closed
   2. Tripped/Closed
   3. Alarm/Normal
   4. On/Off
   5. Auto/Manual
   6. Remote/Local
   7. On Control/Off Control
   8. Set/Reset

b. 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. If a device remains in this state for a period more than a threshold value, the same shall be alarmed.

c. Momentary change Detection (MCD): The input to capture the states of fast acting devices such as auto-reclosers.

Commanded changes initiated by supervisory control shall not be alarmed but shall generate an event message. All other status changes in the state of telemetered, calculated digital input points & uncommanded changes shall be alarmed. Each CB, switching device etc. shall have normal & off normal positions states defined. In the event of off normal positions, the same shall be reflected in the off normal summary list.

2.2.5.3 Calculated Data processing

SCADA system shall be capable of performing calculations and storing the result in the database as calculated data available for display. The database variables to be used for arguments and the mathematical/statistical/logical functions to be used as operations shall be definable interactively at a console as well as by the programmer using database creation and maintenance procedures.

Calculated analog values shall use database points as the arguments and mathematical and statistical functions as the operations. Functions such as addition, subtraction, multiplication, division, maximum value, minimum value and average value, count, integration, square root extraction, exponentiation, trigonometric functions, logarithms and logical & comparative operators etc. shall be provided.

It shall be possible to calculate running maximum value, minimum value and average value over a time interval (time interval configurable from 5 minutes to 60 minutes). The value shall be reset after the elapse of defined time interval. These values shall be stored with time of occurrence for maxima and minima and the time for averaging.

Calculated status values shall use database points as arguments and combinational logic functions that include the logical, comparative operators such as AND, inclusive OR, exclusive OR, NOT, Less Than, Greater Than, Less Than or Equal To, Greater Than or Equal To, and Equal To, If, else if etc. Suitable rules or operators (such as multi-level parentheses) shall be provided to indicate the sequence of operations in the calculation.

2.2.5.4 Substation Topology Processing

The SCADA system shall be provided with a Substation topology processor function. This function shall be capable of analyzing the open/closed status of switching devices, such as breakers and disconnectors, in order to define the configuration of the substation for display. The energization of lines, transformers, bus sections and generating units shall be determined so that the associated displays may correctly show the status of these power system elements. The configuration shall be re-evaluated and updated whenever a switching

device status change & analog value change beyond dead band is detected.

2.2.5.5 Alternate source for data:

The system shall have capability to accept multiple data sources by defining as main & secondary. Normally, data from normal source will be considered. In the event of non- availability of primary source, data from secondary source shall be considered & once primary source is healthy, it shall switch back to primary source. There shall be an indication for primary /secondary source in displays, reports etc. Suitable alarm shall be generated in the event to change from primary to secondary & vice versa. Alternate source of data can be defined for certain critical points in the database.

2.2.5.6 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.

The quality of the calculated value shall be the quality of its "worst" component of its arguments. The presence of a quality code on any of the component data values shall not disrupt the calculation using that value. 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 replaced quality code from one of its component values.

At least the following data quality codes preferably as the following single letter code shall be provided. However, distinct symbols /shapes after approval from NEA may also be used.

S. No.	Quality code	Code	Reason
1.	Telemetry Failure (RTU Link)	T	Telemetry has failed
2.	Manual Replaced	M	Manual updation
3.	Delete from Scan (RTU/point)	D	User disabled the scan of the of data/point
4.	Questionable data	Q	Analog values of the de- energized elements
5.	Calculated	C	Calculated data
6.	Estimated	E	Estimated data from state estimator
7.	Limit Override	L	Limits are overridden
8.	Primary /secondary source	P/S	Primary or secondary source
9.	Reasonability Limit Exceeded	R	Value beyond reasonability limit
10.	Alarm Inhibit	A	Alarm processing is inhibited
11.	Test or maintenance mode	X	Point is in test /maintenance mode

2.2.6 Continuous Real-time data storage and playback

All real-time data (Analog and status) shall be continuously stored in auxiliary memory for at least two weeks as and when it is received in the SCADA database from the RTUs.

It shall be possible to playback above stored data on single line diagram and network diagram for a time window of at least 10 minutes (configurable in seconds /minutes) by defining start and End date and time. It shall be possible to have tabular and graphical trends of the stored data. It shall be possible to set a different sampling rate for playback than the sampling rate for data storage.

The users shall be able to select the time window of interest for archival of data in the ISR system for future retrieval and playback in SCADA system. This archived data shall be transferable in RDBMS database tables of ISR system for generation of tabular displays and reports.

2.2.7 Sequence-of-Events data

Sequence-of-events (SOE) data shall be chronological listings of „status change events with time stamp" acquired from RTUs. The SOE data shall be collected from all RTUs either in normal polling or periodically/on demand. SOE data collection shall have lower priority than supervisory control actions and normal data acquisition. The SOE data collected from different RTUs shall be merged for chronological listings and stored for subsequent review. At least latest 1000 SOE data shall be available for display.

The SOE resolution of RTU is defined in respective sections for RTU. SCADA system at control center shall have 1ms SOE resolution. However, as SOE time stamping is done at RTU level, the same shall be in line with resolution defined for RTU.

All SOE data collected from all RTUs shall be stored in daily RDBMS database of ISR system.

2.2.8 SCADA language

The SCADA system shall have capability to write various programs using IEC 61131-3 SCADA language or C/C++ or any non-proprietary language. It will facilitate user (programmer) to write

various programs/ logics using points defined in the database.

2.2.9 Supervisory Control

The operator shall be able to request digital status control, set-point control and raise/lower control on selected points and analogs using Select check before operating (SCBO) Sequence. Supervisory control shall allow the SCADA system to remotely control switching devices. A control action shall require a confirmation-of-selection-prior-to-execution response. Initiation of the control execute step shall occur after the dispatcher confirms that the correct point and control action have been selected.

After the dispatcher function initiates control execution, the RTU shall be addressed for verification that the correct point has been selected at the RTU and then the control action shall be executed.

It shall be possible to issue control commands as a group control from SCADA where switching devices pertaining to different RTUs or a RTU may be controlled as a group. The SCADA system shall send the control commands sequentially (without dispatcher intervention), if the commands pertain to switching devices in the same RTU, using the Selection Check before operating (SCBO) of prior–to-execution. The control commands pertaining to different RTUs may be executed in parallel.

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 action other than completing the control action, the selection shall be cancelled, and the user be informed. If the communication to the RTU is not available, the control command shall be rejected and shall not remain in queue.

The user shall not be prevented from requesting other displays, performing a different supervisory control action, or performing any other user interface operation while the SCADA system waits for a report-back on previously executed control actions.

The system shall process supervisory control commands with a higher priority than requests for data from the RTU data acquisition function.

Functional requirements for the various types of supervisory control are given below. A supervisory control request shall be sent from control center only after the controlled point was checked for proper conditions. The request shall be rejected by the System if:

1. The requested control operation is inhibited by a tag placed on the device or maintenance tag.
2. The device or S/S in local manual control mode.
3. An Uninitialized, Telemetry failure, delete from scan, manual replaced, Test/maintenance, or Manually Entered data quality indicator is shown for the device.
4. The Operating Mode/ user permission of the workstation/console attempting control does not permit supervisory control
5. The device is already selected for control request or control execution is from another workstation / user/window /console or control request is progressing
6. Time out after selection
7. The device is not subject to supervisory control of the type being attempted

Rejection of a control request from control center shall occur before any transmission is made for control purposes. A control rejection message shall be displayed for the Dispatcher.

2.2.9.1 Digital Status Control

A digital control output results in the activation of an output relay in RTU. Different commands shall be possible for these digital status controls.

Successful completion of the control request shall be recorded as an event. Failures to complete shall be handled as specified in UI section. Control requests shall be canceled and the selection of the point shall be terminated when the user cancels a request, does not perform the next step of the control procedure within the selection time-out period from the previous step of the procedure, or the request is rejected.

2.2.9.1.1 Breakers

The user shall be able to select and operate the two-state controllable switching device i.e. Circuit breakers/ Load Break Switch.

2.2.9.1.1.1 Reset flag

The user shall be able to select and operate switches as per NEA SOP.

2.2.9.1.1.2 Capacitor Banks

The user shall be able to control capacitor 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 that time period & dispatcher is required to give command after expiration of inhibited time period.

2.2.9.1.1.3 Tap Changing Transformers

SCADA system shall have the capability to raise and lower the on load tap position of the transformers from SCADA control center through supervisory commands.

Depending on system conditions, the user may raise or lower the tap positions of On Load Tap Changing (OLTC) transformers. OLTC's tap position needs to be monitored if supervisory control action is to be exercised. OLTC tap position input shall be acquired as an analog value. 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. 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 (SCBO) Sequence. Upon receipt of the raise/lower command, the RTU will immediately execute the control action. It shall not be necessary for the user tore-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. This multi-step procedure as described below

1. The RAISE and LOWER pushbuttons shall be displayed.

2. The command shall be launched as soon as RAISE or LOWER is selected.
The Raise and Lower buttons shall not be replaced by a single Execute button. The RAISE/LOWER pushbuttons shall continue to be displayed, and it shall be possible to initiate these controls repeatedly without reselection of the controlled point, provided that the execution of the previous control command has successfully been completed.

3. The RAISE/LOWER pushbuttons shall remain available until either (a) the dispatcher clicks the CANCEL button or (b) the control times out due to inaction by the dispatcher.

4. A separate timeout period, adjustable in the range of up to 120 seconds, shall be provided for incremental control. The timer shall be reset and start counting again whenever a RAISE or LOWER command is issued.

Successful completion of incremental control shall be recorded as an event. However, failure of incremental control, including failure to achieve the intended result, shall be alarmed.

2.2.9.1.1.4 Set point Control

The SCADA shall provide the capability to issue set point control using SCBO procedure to field equipment The SCADA shall transmit a numerical value to the device being controlled, to indicate the desired operational setting of the device.

2.2.9.1.1.5 Auto execution sequence /Group control

The Auto execution sequence function shall permit multiple supervisory control commands to be programmed for automatic execution in a predefined sequence. The dispatcher shall be able to execute this sequence. Commands to be supported shall include:

- Time delayed
- Pause & until a user commanded restart or step execution
- Jump to other sequence on certain conditional logic
- Manual Entry.

After executing a supervisory control action, the SCADA shall pause to obtain an indication of a successful control completion check. If the control completion check is not received, or does not have the expected value, the SCADA shall terminate the execution of the sequence and shall declare an alarm. Apart from waiting for control completion checks, and unless there is an explicit command for a delay, such as a “Pause” or “Stop” command, the SCADA shall not introduce any other delays in the execution of a sequence. No limit shall be placed on the number of Auto execution sequences, which may execute in parallel. At any time during the execution of a list, the user shall be able to stop further execution via a cancel feature.

2.2.9.1.1.6 Control Inhibit Tag

A 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 up to 4 tag types with the following attributes for each:

a) Type of controls that shall be inhibited by the tag (e.g. open only (Green tag) close only (Yellow tag), open and close (Red tag), or information only - no control inhibit (White tag). Tags shall be preferably identified by colors. However, distinct symbols /shapes after approval from

NEA may also be used.

b) Tag priority

Further the user shall be able to place at least 4 tags per device. 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.

When a tag is placed on a device, the user shall be prompted to enter tag number and comment. An event message shall be generated each time a control inhibit tag is placed or removed with information on user ID, type of tag, time of placement or removal of tags.

2.2.9.1.1.7 Control Permissive interlocks

It shall be possible to define the interlocks at SCADA level as necessary for control actions. It shall also be possible for operator to bypass the interlock which shall be recorded as an event message with user ID information.

2.2.9.1.1.8 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 of 1 to 60 seconds (adjustable in steps of one second) shall be supported, any of which may be assigned to any device.

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:

(a) The control message exchange was not completed successfully,

(b) The device failed to operate, or

(c) 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. For commands issued as part of a group control applications. 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 devices in the group that failed to operate.

2.2.10 Fail-soft capability

The SCADA system shall be able to manage & prevent system from total shutdown / crash etc.in the event of system crosses mark of peak loading requirements through graceful de- gradation of non –critical functions & also relaxing periodicity / update rate of display refresh & critical functions by 50%.

2.2.11 Remote database downloading, diagnostics & configuration

The SCADA system shall be able to download database run diagnostics & create/modify /delete configuration/ parameterization from centralized control center locations to RTU etc. using ASDU/ messages of respective protocols or file transfer.

2.2.12 SCADA Data Analytics

SCADA data analytics is envisaged for the analysis of all types of substation feeders across the NEA substation network, with outcomes presented through a dashboard to facilitate quick analysis and effective decision-making.

The tool should be capable of

a) Reports for analysis of substations along with tripping details
b) Current analysis at feeder level.
c) Voltage analysis for the network.
d) Alarms segregation and analysis
e) Power Quality, network power factor.
f) Historical analysis of different parameters its relation SCADA Data preprocessing using data mining technique involving transforming raw data into an understandable format.
g) Real-Time Grid Monitoring
h) Energy Loss and Theft Detection
i) Load Forecasting and Demand Management
j) Power Quality Analytics
k) Alarm and Event Analysis
l) Performance Benchmarking and Reporting
m) Cybersecurity Monitoring
n) Visualization and Custom Dashboards

The dashboards shall be dynamically configurable with the provision for arithmetic and logical operations on selected datasets ex: adding transformer load, selecting the feeders/transformers/lines having load greater/lesser than user defined value. The Dashboards shall be configurable for the following:

a) Feeder level analysis Dashboard

b) Substation Power Transformer parameters analysis

c) Substation /Grid level Event /status analysis

d) Behavior modelling of Measured & Event/status parameters for Transformer optimal usage

e) Analytical outcome for feeder tripping

2.3 Information Storage and Retrieval

Information Storage and Retrieval (ISR) function shall allow collection of data from real-time SCADA system and storing it periodically in a Relational database management system (RDBMS) database as historical information (HI) data. This includes storing of data such as SOE, status data, Analog values, calculated values, Energy values etc. Programmer shall also be able to set storage mode as by exception in place of periodic storage.

Subsequently, the data shall be retrieved for analysis, display, and trending and report generation. All stored data shall be accessible from any time period regardless of changes made to the database after storage of that data (e.g., it shall be possible to retrieve stored data for a variable that no longer exists in the SCADA computer system through backups on storage medias viz. tapes /MO disks e t c .

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.

It should be able to compress data and should have 100% retrieval accuracy. However, the retrieval of compressed historical streams should be of the same performance levels as normal SCADA retrieval. The ISR should be able to interface over ICCP, OPC, ODBC and

CIM/XML, JSON to external systems **(as defined by NEA to interface within the section "Data exchange")** for analytics over SOA / ESB for Integration with IT Systems, over the Enterprise Services Bus & SOA Architecture provided as part of legacy system. The ISR system shall act as the real interface between SCADA and IT System, where-by the real-time operational system is not affected with a transaction processing system like IT, and the IT Integration efforts will not in any way effect the real-time operationally of SCADA System.

In ISR should also support ad-hoc queries /reports and define display and report formats for selected data via interactive procedures from operator workstations. Formatted reports and responses to user queries shall be presented in alphanumeric or graphical format on either operator workstations or printers at the option of the user. Procedure definition facilities shall be provided for activities that will be frequently performed. SQL-based language shall be used for selecting, retrieving, editing, sorting, analyzing, and reporting ISR data stored. The selection and sorting criteria shall include time tags and ranges, station names, point names, equipment types, status values, text string matches on selected data fields etc. and combinations of these criteria.

It shall be possible to reload any IS&R archival media that has been removed from IS&R and access the archived data without disturbing the collection, storage, and retrieval of IS&R data in real-time.

The ISR system shall also be used for mass storage of data/files such as continuous real-time data of selected time window etc.

The online period of data tables is 24 months, however, there shall not be time restriction to online availability of logs, real time data based on the stored values.

2.3.1 Circuit breaker status Table

The ISR function shall maintain a table in RDBMS database where real-time status of all Circuit breakers along with the associated quality codes shall be stored. The change of status of any breaker shall be updated in this table as soon as the change is detected by the SCADA system. This table shall contain additional information such as date & time of tripping, cause of tripping, Expected duration of outage etc. Some of the causes of tripping could be Supervisory control by user, Protection tripping, Tripping & closing. For expected duration of outages due to protection tripping, the same shall be user enterable field. Such daily tables for 24 months duration shall be stored on auxiliary memory (Online). Tables for the previous day shall be backed up to Magnetic tape/or any offline storage device for this purpose by the user at 10AM daily.

The ISR function shall transfer the information available in the "Circuit breaker status table" as defined above and may be used by existing legacy system using SOA/Enterprise Service Bus, over ODBC/OPC/ICCP Adapters/Interfaces.

2.3.2 Real-time Database Snapshot Tables

At the end of each 5 minutes, the following real time snapshot data shall be stored in RDBMS **in Real-time Database Snapshot tables:**

a) All telemetered analog values and Calculated values for all tele-metered analog points (at least maxima & minima with associated time and average values). Energy values are not envisaged for storage in Data snapshot tables.

b) All status values with time stamp

All the above values as specified above in (a) & (b) shall be stored along with their associated quality code. The periodicity of the snapshot shall be user adjustable to include 5, 15, 30, and 60 minutes. Data Snapshot tables shall be created on daily basis. Such daily tables for 24 months duration shall be stored on auxiliary memory (Online). Tables for the previous day shall be backed up to Magnetic tape/ or any offline storage device for this purpose by the user at 10AM daily.

The ISR function shall prompt the user through a pop-up window to inform the user for taking the backup. The pop-up window shall persist till user acknowledges the same. In addition to that data can be stored on offline storage device.

The user shall also be able to initialize the study-mode power system analysis functions from stored snapshot data.

2.3.3 Hourly Data tables

At the end of each hour information as defined below shall be included in the hourly data tables, in RDBMS database form:

(a) Selected analog values along with their associated quality codes

(b) Selected status values along with their associated quality codes

(c) Results of hourly calculations for selected analog points (atleast maxima & minima with associated time and average) along with their associated quality codes.

(d) In addition to above a separate hourly energy data table exclusively for energy values (Export and Import Active and reactive Energy values for each feeder) shall be created in ISR along with their associated quality codes.

Hourly data tables shall be created on daily basis. Such daily tables for 24 months duration shall be stored on auxiliary memory Online). Tables for the previous day shall be backed up to Magnetic tape/ or any offline storage device for this purpose by the user at 10AM daily. The ISR function shall prompt the user through a pop-up window to remind the user for taking the backup. The pop-up window shall persist till user acknowledges the same.

2.3.3.1 Missed Hourly Data Storage

The programmer shall be able to independently assign any one of the following processing for each hourly value to be executed when the value is missed and cannot be acquired prior to the storage of hourly values.

a. Store zero and a telemetry failure quality code for each missed hour.
b. Store the last good data value, with a questionable data quality code, for each missed hour.
c. Temporarily store zero with a telemetry failure code for each missed hour.
d. When the next good hourly value is obtained, divide that value by the number of hours since the last good value was obtained and insert this value, with a questionable data quality code, for all hours with missed data and the first hour that good data was obtained as is the case for energy values

2.3.3.2 Hourly Data Calculations

The programmer shall be able to define calculated values using stored hourly data and constants as operands. The calculations shall allow the carry-forward of data from one day, week, or month

to the next. The results of all calculations shall include quality codes derived from the quality codes of the operands. The following calculations shall be provided:

a. Addition, subtraction, multiplication, and division

b. Summation of an hourly value by day, week, and month: The running total of the summation for the current day, week, and month shall be updated each hour and made available for display.

c. Maximum and minimum of a value over a programmer-definable time period and the time the maximum or minimum occurred

d. Average of a value over a programmer-definable time period

2.3.4 Daily Energy Data table

The daily energy data table shall be generated for storage of daily energy values for 15 minute blocks / one hour blocks of a day & shall be stored for each feeder on daily basis along with quality codes. This table shall be created on daily basis. Such daily tables for 24 months duration shall be stored on auxiliary memory. Daily Energy data table for the previous month shall be backed up to Magnetic tape by the user on the 10th of every month.

2.3.5 Load priority table

ISR system shall maintain a Load priority table containing information such as breaker name, number of consumers connected to each Breaker and Load priority of each Breaker. There shall be suitable alarm/event message including user ID for such activity.

2.3.6 SOE data table

ISR system shall maintain SOE data table which shall store the SOE data for complete substations. It shall be possible to sort the table by Time, Date, Substation name/, feeder/line name, device name etc. using SQL commands. This table shall be made on daily basis. Such daily tables for three years duration shall be stored on auxiliary memory. For the purpose of sizing of table, daily 4 changes per SOE point may be considered. All CBs, protection and alarm contacts shall be considered as SOE. Tables for the previous day shall be backed up to Magnetic tape/ MO disks by the user at 10AM of every day.

2.3.7 User defined index table

ISR system shall maintain record of user defined indexes derived for performance from telemetered data to record on daily weekly monthly, quarterly, yearly basis. Such daily tables for three years duration shall be stored on auxiliary memory. Tables for the previous day shall be backed up to Magnetic tape/ MO disks by the user at 10AM of every day.

2.3.8 Average time restoration table

ISR system shall maintain record of avg time to report outage location, restoration of supply of feeder, project area on monthly, quarterly, yearly basis. Such daily tables for three years duration shall be stored on auxiliary memory. Tables for the previous day shall be backed up to Magnetic tape/ MO disks by the user at 10AM of every day.

2.3.9 Daily /Weekly Flash report for management of NEA

ISR system shall maintain record and flash report in form of dashboard for management of NEA

exhibiting key performance indices. Such daily tables for three years duration shall be stored on auxiliary memory. Tables for the previous day shall be backed up to Magnetic tape/ MO disks by the user at 10AM of every day

2.3.10 Historical Information (HI) Data Retrieval

The data stored in the ISR system shall support the following retrieval capabilities:

a. The user shall be able to view and edit HI data on displays/Forms and reports. The user shall be able to edit HI data, request recalculation of all derived values, and regenerate and print any daily, weekly or monthly HI report for the current and previous month.

b. The user shall be able to view tabular trend and graphical trend of multiple data points simultaneously by specifying the start date and time, the end date and time, and the time period between displayed samples. The duration of viewable tabular trend and graphical trend could be up to 24 hours. The features of Tabular/graphic trend are mentioned in the specification for User interface.

c. The HI retrieval shall expose the ISR Data over SOA / Enterprise Services BUS over CIM/XML, ICCP or OPC ODBC Interfaces / Adapters.

d. The retrieval shall provide 100% accuracy and fidelity of data

2.3.11 System Message Log Storage and Retrieval

System message log, which shall consist of the chronological listing of the SCADA computer system alarm messages, event messages and user messages shall be stored for archival and analysis. Each entry shall consist of time tag and a text containing user and device identification as displayed on the Alarm Summary or Event Summary displays. The System message log data storage shall be sized for up to 20,000 entries per month.

System message log data shall be stored in daily tables & shall be available for minimum two months on auxiliary memory (online) System message log data for previous months shall be Backed up on Magnetic tapes/ MO disks by the user for which ISR function shall prompt the user every hour with suitable message to remind user for taking the backup on the 10th of
every month. This message shall be disabled once the backup is taken.

Facilities to sort and selectively display and print the contents of the system message log shall be provided. The user shall be able to select the display of system message log entries based upon Alarm type, Events, User generated messages, Device, and Time period.

2.3.12 Mass storage of data/files

The ISR system shall be sized for mass storage of data/files .

2.4 Load Shed Application (LSA)

The load-shed application shall automate and optimize the process of selecting the best combination of switches to be opened and controlling in order to shed the desired amount of load. Given a total amount of load to be shed, the load shed application shall recommend different possible combinations of switches to be opened, in order to meet the requirement. The despatcher is presented with various combinations of switching operations, which shall result in a total amount of load shed, which closely resembles the specified total. The despatcher can then choose any of the recommended actions and execute them. The recommendation is based on Basic rules for load shedding & restoration

In case of failure of supervisory control for few breakers, the total desired load shed/restore will not be met. Under such conditions, the application shall inform the dispatcher the balance amount of load to be shed /restore. The load-shed application shall run again to complete the desired load shed /restore process. The result of any Load Shed operation shall be archived in Information storage and retrieval (IS&R) system.

2.4.1 Basic rules for load shedding & restoration

The load shall be shed or restored on the basis of following basic rules:

(a) By load priority

The LSA shall have a priority mechanism that shall allow the user to assign higher priorities for VIP/ Critical loads or any other important load or feeders. The load assigned with the higher priorities shall be advised to be shed later and restore earlier than load with relatively lower priorities. Each load priority shall be user definable over the scale of at least 1-10.

(b) **By 24 Hrs. load shed /restore history**

The loads of equal priorities shall be advised for restoration in such a way that loads shed first shall be advised to be restored first. The application shall ensure that tripping operations is done in a cyclic manner to avoid the same consumers being affected repeatedly, however, priority loads shall be affected least.

(c) By number of consumers affected

The consumer with equal priority and similar past load shed history shall be considered by the application in such a way that minimum number of consumers are affected during the proposed load shed. The data for number of consumers connected to a feeder /device shall be taken from computerized system.

2.4.2 Modes of operation

The load-shed application shall operate in the following modes:

(a) Manual load shed

(b) Manual load restoration

(c) Auto load shed

(d) Auto load restoration

Each mode of operation can be enabled or disabled by operator independently. The load can be shed & restore in possible combination i.e. manually shed & auto restore vice versa or both operations in the same modes.

2.4.2.1 Manual Load Shed

In this mode operator specifies a load to be shed in a project area The software shall determine & propose all the possible combinations of switches to be operated for the requested load shed considering the basic rules for load shed & restoration.

In case more than one options are possible, then the application shall identify all such options with the priority of consumers along with the number of consumers are likely to be affected for the particular load shed option. The despatcher shall select & execute one of these options for affecting the load shed.

2.4.2.2 Manual Load Restoration

In this mode operator specifies the desired load to be restored. The software shall determine the switches to be operated for the requested load restore considering the basic rules for load shed & restoration.

In case more than one options are possible, then the application shall identify all such options with the priority of consumers along with the number of consumers are likely to be restored for the particular load restore option if chosen by despatcher. The despatcher shall select & execute one of these options for effecting the load restoration.

The Load shed Application shall maintain a load restore timer, which shall automatically start after tripping of CB due to manual load shedding. An alarm shall be generated to remind the operator to restore the loads when this timer expires. For manual mode of operation, the dispatcher shall enter the value of load restore timer.

2.4.2.3 Auto Load Shed

This shall have two modes namely frequency based load shed & time of day based load shed as described below.

(a) Frequency based Load Shed

The function shall execute the tripping of breakers based on the system frequency automatically considering the basic rules for load shed & restoration.

The software shall automatically execute the switching operations as soon as system frequency reaches at load shed start (LSS_str) frequency threshold and it shall continue to do so unless system frequency crosses the load shed stop (LSS-stp) frequency limit.

The frequency limits shall be despatcher assignable up to single decimal points. Once frequency crosses below LSS_stp limit, then load shed can only be started again when frequency attains LSS_str. Limit LSS_str shall be lower than LSS_stp & suitable protection to ensure that shall be provided in user interface such as discard, forbidden etc. if user accidently enters LSS _str higher or equal to LSS_stp or LSS are entered higher than LSR

(b) Time of day-based Load Shed

The function shall operate to shed load at the predefined time of the day & load to be shed. The software shall automatically execute the switching operations considering the basic rules for load shed & restoration.

2.4.2.4 Auto Load Restoration

This shall have two modes namely frequency-based load restoration & time of day based load restoration as described below:

(a) Frequency based restoration

The function shall execute the closing of breakers based on the system frequency automatically considering the basic rules for load shed & restoration.

The software shall automatically execute the switching operations as soon as system frequency attains load restore start frequency limit (LSR_ str) and it shall continue to do so as long as system frequency is crosses below the mark load shed restore stop frequency limit

(LSR_stp). The frequency limits shall be despatcher assignable up to single decimal points. Once frequency crosses below LSR_stp limit , then load shed can only be started again when frequency attains LSR_str. Limit LSR_str shall be higher than LSR_stp & suitable protection to ensure that shall be provided in user interface such as discard ,forbidden etc. if user accidently enters LSR _stp higher or equal to LSR_str or LSR limits or LSS _str higher or equal to LSS_stp or LSR limits, lower than LSS . The sequence of frequency limits shall be permitted as LSR str>LSR_stp>LSS _stp >LSS_str. Adequate protection as mentioned above shall be given if user tries to violate the same.

suitable protection to ensure that shall be provided in user interface such as discard ,forbidden etc. if user accidently enters LSR _stp higher or equal to LSR_str or LSR limits or LSS _str higher or equal to LSS_stp or LSR limits, lower than LSS . The sequence of frequency limits shall be permitted as LSR str>LSR_stp>LSS _stp >LSS_str. Adequate protection as mentioned above shall be given if user tries to violate the same

(b) Time of day based restoration

The function shall operate to restore load at the predefined time of the day & load to be restored. The software shall automatically execute the switching operations considering the basic rules for load shed & restoration.

2.4.3 Alarms/Events

All Load shed & restore operations executed shall be logged in the system as events. In case the supervisory control fails during the operation in predefined time, an alarm shall be generated with the possible reason for the failure.

2.4.4 Summary Report

Load shed application shall generate Summary Reports for project area on daily basis. These reports shall be available online for minimum period of two days. The following reports shall be made.

(a) Daily Load shed report indicating, substation name, feeder/device name, date /time, duration of load shed and amount of load shed, Number of consumers affected based on consumer indexing information, mode of load shed including planned outages of feeders/network equipments.

(b) Daily Alarm summary pertaining to LSA, substation wise.

(c) Substation wise daily Served, un-served power & energy for every 5-minute time block

(d) Served & un-served power for last seven days for every 5-minute time block to calculate Load forecasting for the next day. The report shall contain a column to define weightage factor (multiplier) by despatcher to calculate Load forecasting for the next day. The weightage factor is required to consider the type of the day such as holiday, festivals, rainy day, etc. Separate report for total load forecast of complete project area shall also be generated from above two reports.

2.5 Distribution Load Forecasting

Short-Term Load Forecasting (STLF)

Short-Term Load Forecasting (STLF) analytical function will be used for assessment of the sequence of average electrical loads in equal time intervals, from 1 to 7 days ahead or can be

extended for 1 month if required. As noted above, the STLF function shall be based on different forecasting methods such as:

- Autoregressive.
- Least Squares Method
- Time Series Method.
- Neural Networks.
- Kalman filter
- Weighted Combination of these method

In the first step, training module is executed using load data series from the historical database and weather conditions. After appropriate training, forecast module is executed for up to next 7 days including weather forecast. Results are available in tabular and graphical form. The user shall be able to adjust the active forecast. The adjustments can also be done through weather conditional data parameters i.e. temperature, humidity, precipitation level, wind speed, wind direction acquired through telemetered sensors or manually.

STLF will be used for forecasting of loads for the next short-term period (up to 7 days), to provide planning of the (optimal) network operation at the daily level. in periodic time (15 min to 1hr).The user shall be able to save forecasts in save cases, one of which shall contain the active forecast that shall be available for study functions.

Similar day forecasting

A similar day forecast shall be used that is based on the normalized half-hourly load values stored for each of seven-day types. Provision shall be made for storing day types for the last 24 months. The storage shall be updated each day by replacing the oldest of the same day type with the most current actual load curve.

The similar day forecast shall search the 24-month file for the same day type whose weather conditions best match. It shall then present the user-entered and best-matched conditions, for user comparison, together with the chosen day's loads as the suggested forecast. The user shall be able to modify any of the forecast's loads manually. In addition, the user shall be able to scale the entire forecast by simply specifying an appropriate peak load value. Multi-day forecasts shall be constructed by permitting the user to define the input data for each forecast day. The results of the previous forecasts will be compared with the actual load realization. The performed differences will be used for updating the forecasting procedure parameters.

Results of Function

a) Main input data for the LF will be:

- Historical Load measurements for specified network points, associated with corresponding weather conditions.
- Daily load curves & energy consumption from the past, for all type of days and seasons.
- Weather prognosis for the forecasting period.

b) Main output data of the STLF will be:

- Forecasted load for the forecasting period

2.6 Common Disaster Replica Recovery Centre (DRR)

The same shall be replica of SCADA Control center and with secured permission and upon non

availability of main SCADA Control center. However, system shall remain in sync at hourly basis and shall be suitable interlocks to avoid any accidental command. In case main control center is not available, all underlying equipment i.e. RTU etc shall switch reporting to DRR and DRR will now act as master and sych old master. The process of switching shall not take more than 15 minutes. Now, after swapped configuration of DRR and Main Control Centre, the data sych shall continue from new master SCADA Centre to swapped DRR centre.

2.7 Data recovery function (DR)

The DR function is a repository of system build up software. Three year online backup shall be available at this location with data pertaining to each area i.e. system build ups shall be available of each area separately so that the same can be utilized upon setting up newer system after disaster. The data related to network model of SCADA control center of each area shall be sent to DR center (backup control center) periodically once a day & upon user request. The data shall be configured to be sent globally & incremental. All logs, data model etc. & necessary interfaces that are essential for complete system build up shall be stored at DR center (backup control center). All requisite data which is build the system from scratch shall be transferred to DR. An alarm shall be generated & send to SCADA control center upon attaining user defined threshold e.g. 80% for storage at DR center (backup control centre).

2.8 Historian Data Requirements

The SCADA expansion project shall require a robust and scalable data historian system to capture, store, analyze, and visualize operational data from substations in real-time and historically. The historian shall support both real-time data acquisition and long-term historical data archiving, enabling detailed analytics, performance monitoring, and compliance reporting.

The proposed historian system shall support a variety of data types, including time-series data, event-based data, and calculated tags. It must be capable of acquiring data from diverse field sources such as RTUs, FRTUs, IEDs, SCADA systems, and AMI meters using industry-standard communication protocols such as IEC 60870-5-104, Modbus, or OPC-UA.

The system should be capable of handling high-frequency data ingestion, with a scalable architecture to accommodate increasing data volumes as the system expands. Long-term data retention must be supported for a minimum of seven years, with provisions for extension in accordance with regulatory or operational requirements. The historian shall incorporate dynamic, user-configurable data compression to optimize storage efficiency without compromising data integrity.

High availability must be ensured through features such as hot failover and system-level redundancy across geographically distributed nodes. Security features shall include role-based access control, integration with enterprise identity systems (such as LDAP or Active Directory), and end-to-end encryption for data at rest and in transit. The system must integrate seamlessly with the Distributed Control Centre (DCC) and Backup Control Centre (BCC) SCADA systems to extend analytics and visualization capabilities.

Time synchronization shall be compliant with NTP standards and support nanosecond-level timestamp accuracy to ensure precise data alignment across distributed sources. Archiving functionality must include both automatic and manual options, along with comprehensive backup and restore capabilities for reliable data recovery.

The solution must be scalable for multi-site deployment, supporting a centralized historian architecture with distributed data collectors. It should offer advanced alarming and event-handling

capabilities through Event Frame generation and analytics-based triggers. Data quality must be rigorously maintained through good/bad status tagging, detailed status codes, and complete audit trails to meet regulatory and operational transparency requirements.

2.8.1 Real Time Historian

Real time Historian shall capture high-speed process data (from sensors, meters, IEDs, RTUs) in near real-time for operator dashboards, alarms, and live monitoring in milliseconds to seconds resolution.

2.8.2 Historical (Archival) Historian

Stores time-series data for long-term (seven years) retention, trend analysis, reliability studies, and performance KPIs.

2.8.3 Analytics for operations and management using historian data

a) Real-time energy analytics
b) Equipment health monitoring (transformers, breakers etc.)
c) SCADA event and alarm trend analysis
d) Load forecasting using historical trends
e) Power quality and reliability analytics.
f) Integration with ML/AI platforms for predictive maintenance

-----End of Chapter 2----

CHAPTER 3: USER INTERFACE REQUIREMENTS

3.0 General Requirements

This chapter describes the User Interface requirements for the SCADA system. All SCADA functions shall have common user interface as user interaction shall be performed from Operator Consoles envisaged in this specification. All user interactions shall be from full graphics display.

3.1 System Users

The term "user" is applied to the personnel interacting with the SCADA system. These users shall be required to login in one or more of following **user modes**, which include:

(a) **Supervisor**: Personnel responsible for SCADA 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 as per assigned domain in AoR (Area of Responsibility)
(c) **Engineer:** Personnel having access to certain SCADA system functions and maintenance of database/ displays and responsible for support activities such as post fault analysis, report generation, regular backup of database
(d) **Programmer:** Personnel responsible for continuing development and maintenance of the SCADA system functions, databases, displays and report formats. Security system
(e) **Remote VDU user:** Personnel having only monitoring access of real-time power system from SCADA system, reports.
(f) **DTS (Instructor & Trainee modes):** The Consoles dedicated for DTS shall have instructor & trainee modes.

The role, accessibility for each mode is defined as above, However, the NEA with login as supervisor shall be able to assign the operation of certain functions, or features of functions, to specific user modes. NEA shall maintain the privileges as specified to each user mode .Each individual user shall be assignable to anyone or more user modes. User access to all SCADA functions shall follow a consistent set of common user access guidelines. A mechanism for defining and controlling user access to the SCADA system shall be provided.

Password security shall be provided for access to the SCADA system, its operating system, layered products, and other applications. Each password shall be validated against the corresponding user information in the database. Users shall have the ability to change their own passwords.

3.2 Function and Data Access Security

After a user has successfully logged on, access to the SCADA functions, displays, reports, and databases 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.

The access security function shall compare the user's assigned operating jurisdiction 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) Executing a supervisory control action

There shall be no restrictions on the assignment of multiple jurisdictions to a console & user or the assignment of a jurisdiction to multiple consoles & users. The access security function shall ensure that each jurisdiction is at all times assigned to a least one console. If a console failure or manual reassignment of jurisdiction results in one or more jurisdictions not being assigned to at least one console, the unassigned jurisdictions shall be automatically assigned to a pre- assigned default console and suitable alarms shall be generated.

SCADA users shall not require additional login (username and password) to the other facility allowed as per operating jurisdictions such as ISR. "Single Sign-On" (SSO) technology be employed (i.e., a user logs on once to the SCADA using individually defined username and password which permits appropriate level of access to all SCADA facilities, including IS&R. Further, the facility should be compatible with enterprise-wide SSO capabilities.

Each log-on and log-off shall be reported as an event. Unsuccessful attempts to log-on shall also be reported as events.

3.3 Windows Environment

The user interface for SCADA system shall be web enabled. The SCADA system displays shall operate within a windows environment and shall conform to the standards contained in the X Consortium's Inter-Client Communications Conventions Manual (ICCCM). The window system shall work with the graphical user interface provided and shall allow windows created on the workstations to communicate with processors equipped with X Windows- compatible software on their respective local area networks (LANs) and with future remote applications over the wide area network (WAN).

Alternatively, the SCADA system can have the user Interface based on Microsoft Windows. The functionality in technical specification related to the GUI features of X- windows, shall be met by available features of Microsoft Windows.

It shall be possible to save window configuration in Rooms. Rooms shall allow each user to configure and save a preferred layout, size, and location of windows and displays. The World Display Features shall provide two-dimensional graphic world displays that a user shall be capable of panning, zooming and rubber banding. The world display features such as Layers, declutter levels, Overlays shall be supported. Displays & navigation on VPS shall be same as on the operator workstations.

The user interface software shall be based on state-of-the-art web-based technology to present interactive, full-graphics views of system data via LAN, corporate intranet or the internet. The same displays shall be used.

It is essential that the same web-based user interface (same navigator, same tools) be available to the operator either for local use in the dispatching center or remotely.

Real-Time Dynamic Graphics and HMI Solutions for C/C++, C# / NET, Java and Web / Mobile is envisaged.

The web technology shall be natively supported by the SCADA product, which means that having the displays shown in the web browser shall not bring additional work to the maintenance engineer at display building time. Nor shall it require additional third-party software products like specific plug-ins.

C/C++, Java and C# .NET libraries for a variety of Windows, Linux/Unix and embedded platforms, with MFC, Qt and Gtk support. z Cross-platform support for a run-time choice of a graphics driver: hardware-accelerated OpenGL or a native GDI. z Web deployment via a client-side HTML5 and JavaScript, or server-side (ASP.NET or JSP. Supported platforms: Windows, Linux, Solaris, AIX, HPUX etc

A vast collection of pre-built widgets - real-time charts, graphs, dials, meters, process control symbols and others – to be provided with the Toolkit. The Graphics Builder may be used to modify widget drawings, create dashboards containing multiple widgets, as well as design custom widgets and add them to the Builder's palettes.

The web user interface shall support and enforce all security features including cyber security compliances.

3.4 Display interactions

Rapid, convenient, and reliable display requests shall be provided using the following methods:

3.4.1 Display Requests

a) Selection of a display from a menu display

b) Cursor target selection on any menu, graphic, or tabular display

c) Selection of an alarm : in this case, it shall call up the one-line display containing the alarm's location,

d) Selection of an alarm or event message on a summary display followed by a display request command

e) Selection of display by Entering a display name or number

f) Forward and reverse paging in a page-based display.

g) Selecting a previous display by re-call command.

h) Selecting a point of interest from an Overview display for viewing on full screen (such as viewing a SLD of a substation by selecting the Substation node from a Network diagram).

i) Selecting function keys or cursor targets dedicated to displays.

3.4.2 Display navigation

Display navigation methods shall provide a consistent approach for moving within a display. The following methods shall be provided:

a) Panning with cursor positioning device or scroll bars

b) Zooming with cursor positioning device

c) Navigation window for rapid movement between portions of a world display

d) Rubber-band zooming.

e) Tool tip

f) Find & locate

g) Drag & drop

Zooming shall affect the magnification level of the data displayed. Panning shall move the viewed

portion of a world map space. The size of the viewed portion of the map relative to the whole display shall be indicated by the width of the sliders in the scroll bars of the window displaying the sector. When a display is first called up in a window, it shall be automatically scaled as per default zoom level.

Both continuous and discrete panning and zooming control shall be provided. Continuous panning and zooming shall be done in a convenient and intuitive way using the mouse; and the resulting changes in the screen contents shall be "smooth" and instantaneous without any noticeable delay. Discrete panning and zooming in larger steps shall be possible by dragging the mouse, using the keyboard, and clicking on pushbuttons on toolbars.

When only a part of the display is shown in the active window, the user shall be able to request a "navigation" window for orientation. This window shall show a small replica of the complete display, with the displayed sector of the display highlighted. The user shall be able to move the navigation window anywhere on the screen and shall be able to close it.

A decluttering mechanism that defines the visibility of a graphic construct as a function of its magnification shall be provided. As zooming changes the magnification of data displayed, the declutter mechanism shall cause levels of detail to be shown or suppressed.

The magnification range corresponding to each declutter level shall be defined as system configuration parameter. Static and dynamic elements within a display shall have associated with it a visibility designation as yes or no for each

In addition to reaching the various decluttering levels through zooming, users shall also be allowed to request a specific level from a dialog menu.

The user shall be able to scale (zoom) the image of a world co-ordinate space or display in a smooth fashion to any convenient scale factor. The scale factors shall allow the presentation of an entire world co-ordinate space or display on the full screen or a window.

Static and dynamic data shall be displayed and updated during a scaling operation, and display text shall be scalable to be consistent with the scaled image. At defined scale factors, levels of de-clutter shall be invoked.

The user shall be able to select an area of a world co-ordinate display by cursor manipulation ("rubber-banding") and cause the display to be redrawn with the selected area centered in the display and with the selected area magnified to best fit the full window. The window dimensions shall not be changed by such an action.

A tool tip or equivalent method shall be provided for displaying information in English text & numeral upon moving cursor on the device etc.

Find & locate feature to take the user to the online/ network display where the particular component exists.

3.4.3 Permanent Indicators

Several indicators, including those listed below, shall be permanently shown on each SCADA Display screen as minimum:

- Date and Time: Date shall be presented in the format DD/MM/YY.
- Time shall be presented in the format HH:MM:SS with a resolution of one second, and shall be updated once per second.

- Username: Name of the user logged in the SCADA Name of the active server
- Name of the SCADA display accessed
- Name of the display window

3.4.4 Default Screen Layout

It shall be possible for each user to define a personal layout (Rooms) for the screens displayed on the screen(s) of the workstation, i.e. to define a personal default setup of the position, size, and contents of the screens.

The user's default layout shall appear when the user logs on to a workstation. When a dispatcher takes over a new shift by logging on without the previous dispatcher logging off first, the current screen layout shall be preserved. It shall be possible to go to another room layout of the logged-on user at any time.

3.4.5 Display Note pad

User shall be able to place and edit a note on bays, devices etc. 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.

3.4.6 Quality Code and Tag Indication

All displays and reports containing telemetered analog values, device status and calculated values shall have a data quality code associated with each data field. The quality code 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.

A separate indicator shall identify the devices that have supervisory control inhibit tags. When more than one tag is present on a device, the highest priority tag shall be displayed.

3.5 User Interaction Techniques

The user's interaction with the SCADA 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 provided a menu of operations applicable to the selected item. The required operation alternatives include:

(a) Supervisory control

(b) Data entry

(c) Device status entry

(d) Scan inhibit/enable

(e) Tag placement/removal

(f) Trend.

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. It shall not be necessary to select an execute command to complete the interaction except for supervisory control actions.

The user shall be able to end the interaction sequence at any time by selecting a cancel command.

The progress of all user operations shall be monitored. If the user does not complete to a step within a multi-step operation within a pre-defined time, the process shall reset, and the user shall be informed of the reset. A partially completed action shall be reset if the user begins another non-related sequence.

A programmer-adjustable time-out cancel shall also be provided.

3.5.1 User Guidance

The SCADA 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. User shall be guided for multiple options. The use of mnemonics is prohibited, unless the mnemonics are industry-accepted or approved by NEA. Provisions are required for administrators to edit the toolbars and menus, user guidance messages and to construct new ones through an interactive procedure and without programming.

3.5.2 User Help

In addition to the user guidance, general and specific context-sensitive on-line help shall be available to the SCADA user. Context sensitive means that the help information provided shall be applicable to the next step or steps in the sequence being performed. The Help menu shall present a list of topics available for reference. The topics shall refer to the SCADA user documents. The ability to scroll through the topic's explanatory text shall be supported.

The Help button in a dialog box and help key shall present the text of the user documents where use of the dialog box is explained. The user shall be able to scroll through this text. Exit from the help facility shall return the user to the same point in the sequence for which help was requested.

Context sensitive help facilities shall be provided for each application software package and operator display. The capability to easily edit or add additional help facilities in the future shall be provided.

The provided help facility shall also support:

- Search mechanism
- Navigation links between related topics within the help documents
- Select/copy mechanism
- Print facilities

3.5.3 Overlapping user access

The ability to queue multiple commands from different consoles shall be provided. In this regard, however, interlocks shall be provided to avoid overlapping user access to certain

functions such as data entry and supervisory control as follows:

(a). Data Entry: Although the same data entry field, device status entry or fields (in the case of full-page data entry) may appear concurrently in multiple windows at multiple consoles, data entry for the field or fields shall be restricted to one window at one console at a time. An attempt to initiate data entry for the field or fields from another window shall result in a user guidance message. Concurrent data entry on different areas of a world display, however, shall be allowed.

(b). Supervisory Control: Although the same power system device, such as a circuit breaker, may appear concurrently in multiple windows at multiple consoles, control of the power system

device shall be restricted to one window at a console at a time. An attempt to initiate control of the power system device from another window shall result in a user guidance message.

3.5.4 Function Key Usage

Special functions shall be assigned to the 12 function keys on a standard keyboard. With extensions (e.g., Shift, Alt, Esc) this shall result in a minimum of 48 function key actions.

3.6 Trend

Trend shall be a display of series of values of parameters on a time axis. Both graphical trend and tabular trends shall be supported. The attributes of the trend display shall be user configurable. The trend application shall be able to show trends for any measurement type from more than one source, at least from real- time, historical and forecast sources. It shall be possible to combine this data showing data for comparison using a shared timeline simultaneously comparing for example yesterday (historic) and today (historic, actual and forecast) as two curves on the same time axis. It should be possible to trend different types of parameters (P, Q, V, I, F etc.) with associated Scales on the same display. The user shall be able to select a trend rate different than the sampling rate.

3.6.1 Graphical Trend

The user shall be able to select and configure trending on Graphical displays enabling user for entry of the following parameters:

(a) Data value name

(b) Trend header

(c) Trend direction (horizontal or vertical)

(d) Scale (unidirectional and bi-directional)

(e) Zero offset

(f) Trace number, color & texture

(g) Trend data rate

(h) Trend start time and date (historical data only)

(i) Total trend duration (historical data only)

(j) Reference lines or shading axes (With default to restrictive alarm limits)

(k) Windows/chart to be used

(l) Simultaneous trending of different parameters with associated scales.

Trending of at least four values simultaneously, on a common axis or separate axes shall be supported. All scales corresponding to the values selected shall be visible on the Trend Display simultaneously. There shall be automatic movement of data down or across the screen as new values are generated. 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 & time 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.

When historical data is selected for trending, the user shall be able to page forward and backward, or scroll by the use of a scroll bar, through a non-updating snapshot of the data within the constraints of the data stored in the historical files.

Shading between each trend value and user-definable axes shall be provided. Trend colour shall be changeable based on a comparison of the trend value against associated alarm limits. It shall be possible to have at least data samples corresponding to 2 months online storage foreach of the trended variable. The user shall be able to print the trend without interfering with the continuing trending process.

3.6.2 Tabular Trending

Tabular trending shall be a listing of the time-sequential values of a variable/ variables. 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 variable. The tabular trend shall contain at least rows for samples corresponding to 2 months online storage. Each row shall contain the values of the trended variables. 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 historical tabular trends, which shall be produced from the previously stored values in trend files, it shall be possible to choose the start time, the end time, and the sampling rate independently of the sampled rate of historical data.

It shall also be possible to save trend output to an Excel, .csv ,ASCII file., with date and time information and the engineering unit value of the trended variables for each collection interval. The user shall be able to print the trend on a user-selected printer without interfering with the continuing trending process.

3.7 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) Values returning to normal from a limit violation state

(c) Uncommanded changes of a power system device state

(d) SCADA application program results

(e) Data source communication errors resulting in loss of data

(f) SCADA system hardware or software failures.

Each alarm shall be subjected to a series of alarm processing functions. A device or value's alarmable conditions shall be assigned to an alarm category and alarm priority levels. 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.

All alarm messages shall be recorded on auxiliary memory of SCADA system and archived in chronological order & reverse chronological order. It shall be possible to sort, display and print user selected alarm messages from any console by the user.

3.7.1 Alarm Categories

An alarm category provides the logical interface that connects an alarm condition to a specific Area

of Responsibility (AOR) or operational jurisdiction 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 users. A means shall be provided for changing operating shifts without reassignment of alarm categories at a console. Each log-on and log-off shall be reported as an event.

3.7.2 Alarm Priority levels

Each alarm shall be assigned to an alarm priority level. Up to 8 alarms priority levels shall be supported. Each alarm priority level shall be presented in separate display. For each alarm, it shall be possible for the programmer to independently configure the following actions:

a. Audible alarm tone type selection and its enabling/disabling
b. Alarm messages to be displayed on an alarm summary
c. Alarm message deleted from alarm summary when acknowledged
d. Alarm message deleted from alarm summary when return-to- normal alarm occurs
e. Alarm message deleted from alarm summary when return-to- normal alarm is acknowledged
f. Alarm message deleted by user action.

This assignment shall determine how the alarm will be presented, acknowledged, deleted, and recorded.

3.7.3 User Interaction for Alarms

The User shall be able to perform the alarm interactions described below.

3.7.4 Alarm Inhibit/Enable

Inhibiting alarms for a value or device, including a complete RTU or other data source, shall cause all alarm processing of that value or device to be suspended. The action shall be recorded in the event log. However, scanning of the value or device shall continue and the database shall be updated.

3.7.5 Alarm Acknowledgment

An alarm shall be acknowledged by selecting an alarm acknowledge command when the item in alarm is selected on:

a. Any display showing the item in alarm
b. Any display showing the alarm message.

Use shall be able to acknowledge alarm individually, by page, user selected manner. It shall be possible for the user to distinguish persistent & reset alarms under acknowledged & unacknowledged conditions. All alarms shall be stored by the system.

3.7.5.1 Audible alarm silencing

User shall be able to silence alarm without acknowledgement and shall remain until the user enable the audible alarm. The silencing & enabling shall be recorded as event. The tones shall be definable on the console basis. For each console, multiple tones shall be available. Tones shall be of continuous & short duration type both. The former shall be of high priority condition & require operator intervention to stop. In case of short duration tone, it shall go off at its own.

3.7.5.2 Change Alarm Limits

The user shall be able to change the alarm limits. When the user selects an item to change its alarm limits, a menu showing the alarm limits currently in use and a data entry field for the revised limits shall appear. All changes to alarm limits shall be subjected to data entry error checking and recorded as events. The alarms shall be annunciated according to the changed alarm limits. The user shall be able to reset alarm limits to the limits set in the SCADA database. However, these shall be treated as temporary changes & if the system is re- initialized, the original limits defined in the SCADA database shall be operationalized.

3.7.5.3 Alarm Presentation

Alarm presentation shall be determined by the alarm's category and priority. Displays shall highlight every alarm condition using a combination of color, intensity, inverse video, blinking and audible sound. 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's category.

Alarm messages shall be a single line of text describing the alarm that has occurred and the time of occurrence. The alarm message shall be English text and shall not require the use of a reference document for interpretation.

3.8 Events

Events are conditions or actions that shall be recorded by the SCADA 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.

Events shall be recorded in the form of an event message. The event message format shall be similar to the alarm message format. The same message format shall be used for displaying and printing events. Event messages shall be displayed on an events summary.

Event messages shall be stored on auxiliary memory of SCADA system and archived in chronological order and reverse chronological order. It shall be possible to sort, display, and print event messages from any console.

3.9 Hardcopy Printout

The SCADA system shall have features to produce a printout of a display, reports, Alarms, Events etc. from a menu. Any of the available printers shall be selectable by the

SCADA users from menus for taking printout.

It shall be possible to print a complete display or a selected portion of a display. The options for printing shall include at least choice for orientation, background color, page size, color/black & white and print preview. Also, any of the available printers shall be selectable from the print Menu.

3.10 Report Generation

The contractor shall be required to generate the Daily, Weekly, Monthly reports formats for SCADA system. The report formats shall be finalized during detailed engineering stage. Further modification

,addition deletion of reports as required by NEA is also required to be generated during implementation and FMS The user shall be able to schedule periodic generation of reports, direct report to display, print report, and archive report using report-scheduling display. The report scheduling display shall enable entry of the following parameters, with default values provided where appropriate:

(a) Report name

(b) Report destination (printer or archiving device)

(c) Time of 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 report review displays shall accommodate formatted report pages up to132 characters in width and 66 lines in length and shall contain headings that correspond to the printed report headings. For reports containing more columns or rows than the display, the system shall include a means to view the entire report in a graphic format. The report view and editing displays shall function with the initially supplied reports and all future reports added by NEA.

3.11 System Configuration Monitoring and Control

The user shall be provided with the capability to review SCADA computer system configuration and to control the state of the configuration equipment using displays. The following operations shall be possible:

a. Failover of each server
b. Monitoring of servers, device, including workstations, RTUs status & loading of WAN LANs etc.
c. Monitoring of the processor resource, hard disk & LAN/WAN
d. Utilization
e. Control & monitor of SCADA functions

3.12 Dynamic Data Presentation

It shall be possible to present any item in the database on any display. All supervisory control and data control capabilities shall be supported from any window of a world display. Device status or data values shall be displayable anywhere on the screen, excluding dedicated screen areas such as the display heading.

Only standard X Window system or Microsoft windows standard fonts shall be provided with the SCADA. 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.

Status and data values shall be presented in the following formats as appropriate:

a. Numerical text that presents analogue values shall have the provision for the format definition of the text shall include the number of characters, number of decimal places, and the use of positive /negative sign or flow direction arrows, etc.
b. Normally the telemetered MW/Mvar values along with the sign/direction shall be displayed

on the Single line diagram and Network diagram. However, the user shall also be able to display all other telemetered and calculated/ estimated analog values (I, V, pf etc. for each phase) on the Single line diagram (SLD) and 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. Colors, textures and blink conditions based upon state or value changes or change of data quality, e.g., alarm limits.

3.13 Element Highlighting

Element highlighting techniques shall be provided to draw the attention of Dispatcher to critical state of the system. The highlighting technique shall include change of color, color intensity, blinking, Character inversion, Line texture, appended symbols etc. 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.

3.14 Display Types

The following indicative list describes the types of displays that are to be included in the SCADA system. The user interface shall support the capabilities of all displays as specified. The User mode, Current Time and date shall be displayed on a screen-basis, not on a display basis, and shall be always visible.

3.14.1 Dashboard

A suitable dashboard for NEA to view vital parameters at a glance shall be created.

3.14.2 SCADA System Display

A display shall be provided that lists all SCADA 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.

3.14.3 Substations Network Display

A graphic overview network display of the substations & feeders. The network color coded by voltage shall be provided. This display shall present the distribution system in a graphic format provided by NEA. Telemetered and calculated data like Real and reactive power flows shall be displayed as a value with a direction. Lines that have exceeded their loading limits shall be highlighted. Substations and power stations shall be depicted by symbols that reflect the presence of alarms at that substation or power station. Cursor selection of a substation/ power station symbol shall result in the associated Single line diagram display for that substation/ power station.

3.14.4 Interchange Display

The interchange display shall be provided as a schematic diagram showing power transfers among substations. This diagram shall show each power system as a block with actual and scheduled net interchange values outside the block. Symbolic arrows shall indicate power flow directions. The diagram shall also show schedule deviations. This display shall show the frequency values collected from all substations having tie-lines.

3.14.5 Substation SLD displays Menu

A display shall be provided that lists all substations that can be viewed via a SLD display. 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. Each entry in the list shall have a cursor target for graphic display selection.

3.14.6 Substation SLD Displays

SLD displays shall be provided for each substation, including those for which telemetry may not be available but are required for running the applications. Each display shall present telemetered, manually entered, and calculated power system data on a Single line 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, distribution network 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.

3.14.7 Control panel displays

The control panel displays giving look -alike feeling shall be provided for operator supervise & operate.

3.14.8 Tabular Displays

Tabular displays shall be provided for each substation. These displays shall list the real-time values of telemetered, manually entered, and calculated data associated with the substation as well as related information such as alarm limits. The user shall be able to perform any user interaction defined by the Specification on these displays.

3.14.9 Alarm Summary Displays

Displays 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 at least 200 alarm messages for each alarm summary type. If an alarm summary display becomes full, the oldest messages shall be automatically deleted and the newest messages shall be added. It shall be possible to perform any alarm interaction from this display. The user shall be able to select between viewing events in chronological or reverse chronological order.

3.14.10 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.

3.14.11 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. All summary displays, except for Tag Summary shall be information-only displays; no user interaction, other than display call up, shall be associated with them. The Tag Summary shall be interactive, i.e., the user shall be able to place or remove tags on this summary.

3.14.12 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

3.14.13 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.

3.14.14 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 an RTU 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

3.14.15 Alarm Inhibit Summary

This display shall list devices and data values for which the user has suspended alarm processing.

3.14.16 Tag Summary

This display shall list and describe all active device tags.

3.14.17 Graphical Trending Summary Displays

The summary display shall list all items being trended. The list shall include the item name, trace number or color, trend orientation, and trend range.

3.14.18 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.

3.14.19 Notes Display

This display shall include a minimum of 5 pages on which a user at any console may enter and edit messages. The contents of these pages shall be accessible by any console. The user shall have the ability to clear any page of this display and to type over previous messages.

3.14.20 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

b. Monitor the system's resource utilization statistics

3.14.21 RTU Communication Channel Monitoring and Control Display

This display shall show information on the status of the system's communication interface devices (including communication channels), the accessibility of each RTU in a graphical form. The user shall be able to Enable/Disable any communication channel from this display. Such actions shall be recorded with User ID details

3.14.22 SCADA 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.

3.14.23 SLA monitoring displays

The display shall capture and maintain record and display historical and current values as per requirement of monitoring of SLA.

3.14.24 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.

----- End of Chapter 3 -----

CHAPTER -4: SYSTEM SOFTWARE REQUIREMENTS

4.0 General

This chapter describes the characteristics of system software such as Operating system, RDBMS and support software (programming language compilers, database development and maintenance, display development, network services, report generation, diagnostics and backup utilities) to be provided by Contractor and the original software manufacturer as necessary to support the SCADA applications. This chapter also describes the standards to be followed for all supplied software. It is necessary that functional, availability & performance aspects are met. Bidder shall assess the adequacy of software specified & if any additional software is required to meet all the requirements of the technical specifications, the same shall also be included in the offer.

4.1 Software Standards

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

4.1.1 Design and Coding Standards for SCADA applications

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

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

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

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

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

e. SOA architecture: Software shall conform to SOA.

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

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

Hardware needs technical specification to be specified by the Vendor clearly for this SOFTWARE requirement. Software to be designed as per the I/O requirement below mentioned:

- No. of Substations– 215
- No. of Equipments in each Substation – 29 (Approx Considered)
- No. of DI Inputs – 68370
- No. of DO Commands –8170
- No. of AI Signals (With MFT) – 51600
- No. of AI Signals (Without MFT) – 1720
- No. of Switching Stations – To be proposed by SI after Survey
- No. of additional Equipments – To be proposed by SI after Survey
- No. of additional DI Inputs – To be proposed by SI after Survey
- No. of additional DO Commands – To be proposed by SI after Survey
- No. of additional AI Signals - To be proposed by SI after Survey

Other Application parameters like Accumulated objects, corresponding alarm groups, delay groups, RTU internal events and SCADA server diagnostic events etc. to be considered.

External interface provision for future SCADA based software applications should be made available.

Data Information storage & retrieval shall have retention of minimum 7 years measure and data & 2 years for events data at actual scan frequency of data received through specific / necessary software tools through self or third-party interface software. All the Software/License requirements as per the proposed architecture shall be clearly mentioned during the bidding process. No request of additional licenses will be entertained at the later stages. Necessary License for Historian Database Software's should be provided for generation of front end reports and applications.

4.2 Operating System

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

4.3 Time and Calendar Maintenance

The SCADA system shall maintain Time and date for use by various software applications. The GPS based time receiver shall be used for synchronizing the SCADA system time. All Servers and operator workstation clocks shall be synchronized within the accuracy of +/-100 milliseconds. The SCADA system shall not be dependent one particular server for time /calendar maintenance. . The SCADA shall include two redundant time and frequency standards. Failure of the online unit shall result in automatic switching to the redundant unit. The SCADA shall periodically check if the backup unit is operational and failure of either unit shall be alarmed.

The frequency reading shall be accessible by SCADA applications with three post- decimal digits resolution .The system shall support communication protocols such as NTP and SNTP. The time and frequency standard unit shall support a common time code output format such as IRIG-B.

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

4.4 Network Software

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

4.4.1 Network Communication

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

4.4.2 Network Security

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

The design & configuration, parameterization, placement of DMZ shall be such that SCADA /system shall be protected from intrusion /vulnerabilities from outside world as per IEC62443-2, IEC 62351-3, ISO/IEC27001. The cyber security shall be certified on SAT before Operational acceptance by SI. The same shall be required to be verified at least once annually or Major upgrade or change on the system or data of validity of certification which ever earlier during the FMS period also and maintain required performance and functional requirements/SLA

4.4.3 Network services

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

(a) Network file management and transfer, for files containing text, data, and/or graphics information

(b) Network printing management

(c) Network time synchronization

(d) Network backup over LAN

(e) Task-to-task communications to external computers

(f) LAN global naming facilities.

(g) Remote procedure call

(h) Remote terminal session

4.4.4 Security Services

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

Followings are the functional requirement from the security system:

- System shall have Multilayer (at least network, application layer) firewall which shall protect the complete system network from unwanted users. Further the separate firewall of different OEMs shall be provided to take care the security of all the servers & shall have High Availability architecture with No Single Point of Failure (NSPOF).
- Gateway Firewall should be capable of load balancing multiple links from different service providers.
- LAN Firewall shall provide isolation/security services between the subsystems installed under SCADA system
- Firewalls deployed should not become a bottleneck. It shall be Robust, Secure, Scalable and future proof with Centralized Management.
- Two types of IPS Host based & Network based shall be deployed with minimum hardware & they should not go blind in peak traffics.
- IPS should have hybrid technology to detect attacks. It should detect through a combination of Protocol Anomaly and Signature matching.
- Shall have Gateway antivirus which will protect from inflow of virus from the Internet and other WAN locations at the gateway itself with content filtering without any lag in data transmission.
- Shall have strong authentication containing username and passwords which shall be very difficult to compromise.
- SSL over VPN to provide secured link over public network such as with RTU.

4.4.5 Features

Followings are the features specific to each component of security system

4.4.5.1 Firewall

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

- Firewall speed >250 Mbps
- Firewall including IDS/IPS, Web filtering, VPN
- Data encryption supported DES (56 bits) 3 DES (168 bits) and hashing
- algorithm like MD5 and SHA-1
- Encryption to offload the main CPU or any other standard method to meet firewall
- functional, security & performance requirement
- It shall have minimum 8 Ethernet 10/100 /1000 ports (4ports for connectivity to two web servers & 4 Ports for connectivity to LAN
- Support NAT and PAT
- Capability of working in Load sharing and hot standby mode
- Denial of service prevention.
- DNS guard features
- JAVA and ActiveX blocking
- Radius integration
- Web based management interface

- Stateful inspection for web, mail, SQL application etc.
- Detailed system logging and accounting feature
- No. of concurrent TCP Sessions supported shall be more than 5000.

4.4.5.1.1 Intrusion Prevention System (IPS)

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

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

Automated Update of the signature for contract period shall be provided and there should be provision for creating customized signature

(A) Intrusion Prevention System (Network Based)

After detecting any intrusion attempt there should be provision to configure to perform the following functions:

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

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

(B) Intrusion Prevention System (Host Based)

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

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

4.4.5.1.2 Gateway Antivirus

This shall be used for Gateway scanning of viruses. Gateway antivirus shall have Centralized- user Administration which will Communicate directly with centralized user directories such as

LDAP. It shall have the all the essential/standard features of Latest version of Gateway antivirus, some of the features are as following:

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

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

4.4.6 Other Aspects of Security

4.4.6.1 Application Security Monitoring

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

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

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

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

4.4.6.2 Analysis and Reports

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

4.4.6.3 Log Archiving

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

4.4.6.4 Data Access through intranet

The Web server at Control Center is to function as source of information on the distribution network. It will be accessed by NEA intranet user. Any additional client software, if required, at external clients/users ends, the same shall be made dynamically available from Web server for its downloading by these external clients. There shall not be any restriction to the number of clients downloading this software (i.e. Unlimited number of client downloads shall be provided).

The external users shall be licensed users of the NEA. The following features are required:

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

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

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

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

defining new data/Report/Displays.

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

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

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

h. Suitable load balancing shall be provided among the web servers where each shall serve proportionate number of clients.

However, in case of failure of one of the servers, all the clients shall automatically switch to the other web server(s).

Typical displays/pages for Intranet access shall be same as that on the SCADA**.** Real time SCADA data on web server shall be refreshed every minute. The access to Web server/site shall be controlled through User ID and password to be maintained /granted by a system administrator. Further, different pages/data access shall be limited by user type (i.e. CMD, Mgmt. user, in-charge etc.). The access mechanism shall identify and allow configuration of priority access to selected users.

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

4.4.6.5 Signature Updating Requirements

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

4.4.6.6 Network Management system (NMS)

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

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

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

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

The NMS software shall provide the following network management capabilities:

a. Configuration management
b. Fault management
c. Performance Monitoring

The network management software shall:

a. Maintain performance, resource usage, and error statistics for all the above interfaces (i.e. servers, workstation consoles, devices, telephone circuit interface equipment, and all SCADA gateways , routers etc.) and present this information via displays, periodic reports, and on-demand reports.
b. The above information shall be collected and stored at user configurable periodicities i.e. upto 60 minutes. The Network Management System (NMS) shall be capable of storing the above data for a period of one year at periodicity of 5 minutes.
c. Maintain a graphical display of network connectivity to the remote end routers
d. Maintain a graphical display for connectivity and status of servers and peripheral devices for local area network.
e. Issue alarms when error conditions or resource usage problems occur.
f. Provide facilities to add and delete addresses and links, control data blocks, and set data transmission and reception parameters.
g. Provide facilities for path and routing control and queue space control.
h. SLA monitoring - Availability of all devices shall be monitored and SLA shall be calculated as per SLA requirement specified in FMS chapter.

4.4.6.7 Central Cyber security Monitoring & Detection

The Contractor shall implement a unified cyber security Application platform purpose built to monitor, manage & maintain the security posture of the overall control system network. The system shall establish mechanisms & processes for detection of cyber security threats, to ensure cyber security threats or incidents can be responded promptly to. These shall include key security technologies like central security policy management for host machines, capturing and& analyzing security event logs from all security/networking assets and continuous threat detection systems adopted for an operational technology environment.

The proposed deployment shall be based on a vendor agnostic platform, natively supporting the said cyber security services, while offering flexibility and scalability to provide additional functionalities needed in the context of security improvement plan.

The software platform shall be designed in conformance to key global standards like IEC 62443 and IEC 62351 while supporting compliance to the country specific guidelines/frameworks. The central security management server shall be deployed in the De-Militarized zone inside the control room segregated by suitable firewalls and shall act as an IT/OT interface

All hosts machines shall implement advanced end point protections including antimalware, application whitelisting, data loss prevention, HIPS etc. The whitelisting and application control shall allow only list of permitted applications, services and processes to run on each host; no other processes shall be permitted to be executed on the host. It shall not be possible for users to

circumvent the malicious code protection on a host device.

The Host based IPS shall monitor the characteristics of a host and the events occurring within that host for suspicious activity. The characteristics which need to be monitored include network traffic, system logs, running processes, file access & modification, and system & application configuration changes.

The central policy Orchestrator shall be deployed to enable operators/security administrators to centrally monitor and manage the security policy for all host workstations. The application shall allow creation of automated workflows, support creation of reports, customized dashboards to analyze the performance of each security setting while tracking the

deployment of signature (DAT files) updates date from a single location.

Continuous (24/7) anomaly & threat detection shall be implemented to detect and alert for all known & unknown threats including Zero days, MITM attacks, DDoS attacks, unauthorized behavior or malicious activities on the network. The system shall support a wide range of IT & OT communication protocols including the proprietary protocols, and able to discover information from the network passively using Deep Packet Inspection by connecting to the Mirror Port / SPAN port on a backbone switch(s).

The proposed system shall support the following capabilities:

- **Real time network visualization** of the entire ICS network, including asset inventory information, communication patterns, connections, protocols and topology.
- Discover detailed **asset inventory information** (like Manufacturer, Model, Firmware, serial no. etc.) from network devices including nested devices to enable enhanced visibility, segmentation, and vulnerability management. Additionally, it should be capable of automatic asset grouping to help visualize a micro-segmentation view of the network primarily based on asset behavior.
- Automated **identification of vulnerabilities** in the environment, correlated with operational context to provide detailed insights and rapid remediation.
- The system shall learn typical behavior through **Dynamic learning via artificial intelligence** to automatically learn nodes, devices, connections, etc. to accurately profile normal process behavior and engage a "protection mode" where variants and risks from the learned process behavior are alerted.
- Create detailed behavioral profiles for every device according to the process state thereby identifying/alerting users for anomalies on the network such as new or unusual assets, communication patterns, configuration changes, malfunctions etc. based on extensive learned baselines using **Deep Packet Inspection (DPI) into the OT protocols.**
- System should be able to calculate a **granular Risk score** for each identified threat based on the context it has about the network, the assets and the events that occurred. Automatically capture network traffic associated with the alert to **analyze and identify** what happened before and after the Incident.
- **Integrates with firewalls** to inject rules associated with an alert or policy

The security monitoring application shall encompass collecting security logs from various devices in the system (Hosts, IED's, Firewalls, routers, IDS, AV Servers etc) over standard protocol formats i.e. syslog/SNMP/WMI etc. and provide dashboards for real-time situational security awareness and alerts. The application must be compliant to international standards

IEC62443-3-3 (for providing syslog server and audit trail capabilities) and IEC 62351-14 (for central management functionalities).

The system shall have a capability to archive, record and store all security related events. The logs of the system shall be analyzed for exceptions and the possible incident of intrusion/trespass shall be presented to NEA in the form of alerts/notifications.

The audit log function must be enabled and protected against tampering. The Bidders shall put in place audit trail and logging mechanism to ensure security logs are available for upto 12months.

The entire system shall use a uniform system time which can be synchronized with an external time source (GPS).

The tool must be open and customizable with dashboards as per the local infrastructure requirements and business KPI's. Typically, it should support basic used cases like:

Application Security Monitoring

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

- Application Software Error Conditions
- Application Software Performance Issues
- Application Configuration Changes
- Authentication activities - login, logout, failure access

Host Security Monitoring:

- Security policy changes.
- Anti-malware activities - alerts provided by antivirus or whitelist solutions
- Mobile drive activities - USB connection in the system
- Windows event logs from Windows Machine System - Windows patches and activities,

Network monitoring alerts and events:

- Configuration update activities - settings and parameters changes in systems
- Unauthorized access attempts events from Security appliances

Application must be simple and intuitive to support OT operators with limited IT skills to quickly identity the security issues or any unauthorized access to the system and respond to it before it becomes a major threat to the system. NEA's personnel shall be trained to be capable of creating new custom analysis and reports.

The contractor shall propose a centralized patch management solution to securely execute and manage all necessary systems, security mitigation and signature-related patching in timely manner. All host machines shall be configured via domain policy to contact patch servers and check for missing updates. These updates shall be installed manually to avoid cause unscheduled disruptions.

All the security appliances (Firewalls, Antivirus, central cyber security monitoring & detection appliances etc) being supplied under this project shall have definition updates for virus/signatures and updates for software patches for the warranty and complete FMS period. The

signature and patches shall then be deployed to all the respective devices. These enhancements shall increase security and functionality, without requiring redesigning or reengineering efforts

4.5 Database structure

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

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

The SCADA shall include a single logical repository for all data needed to model the historical, current, and future state of the power system and SCADA – the Source Database (SDB). All information needed to describe the models on which the SCADA operates, shall be defined once in the SDB and made available to all SCADA applications, real-time database, and user interface maintenance tools that need the information.

Any database update, whether due to local changes or imported network model changes, shall be able to be placed online in a controlled manner without causing undue interruption to network operations, including without losing any manually entered data. For example, a network model update to introduce a new substation shall not interrupt the ability to perform supervisory control actions or receive telemetry to view the network state. It shall be possible the changes, local or imported, to be placed online either automatically or under manual control with proper validation. It shall be possible to easily revert to an earlier database Version, again without undue interruption to network operations.

The capability to import & export the CIM compliant network model data including the corresponding telemetry and ICCP data reference in XML format to send it to other parties shall be provided. The capability to import the CIM compliant network model data from other parties in XML format shall also be provided.

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

4.5.1 Software Maintenance and Development Tools

4.5.1.1 General requirements

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

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

The following shall thus be possible:

- Program and data editing

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

Development the following features shall be provided: Library management

- Programs allowing to copy and print any data or program file
- Backup and restore File comparison Sort and merge
- Programs that allow to partially save and recover volumes
- Core and memory dump. In addition, tools shall have the following:

4.5.1.2 Command language

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

4.5.1.3 Linkage Editor and Loader

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

4.5.1.4 Symbolic Debugger

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

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

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

4.5.1.5 System Integration

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

4.5.1.6 System Generation

System generation software and procedures shall be provided to generate an executable object

code of all software, databases, displays, and reports. NEA personnel shall be able to perform a system generation on site, using only equipment, software, procedures, and

documentation supplied with the SCADA. It shall not be necessary to return to the Contractor's facility or rely on the assistance of Contractor personnel.

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

4.5.1.7 Code Management

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

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

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

1. Manage source code and binary images
2. Allow tracking of code changes by date, author, and purpose
3. Manage documentation modules and associate them with source code, binary images, and other documentation
4. Support multiple teams of programmers working concurrently on the same modules
5. Provide an efficient link between modules

4.6 Database Development software

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

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

A Database development software shall be provided which shall contain database structure definitions and all initialization data to support the generation of all relational , real-time database (RTDB) non-relational run-time databases required to implement the functions of SCADA system. All the facilities required for generating, integrating and testing of the database shall be provided with the SCADA system. The delivered SCADA database shall be sized for the ultimate system as described in this Specification. The database

development facility shall be available on development system comprising of server & workstation. Once the database creation/ modification activity is over, the compiled runtime executable shall be downloaded to all respective machines. Executing the database generating functions shall not interfere with the on-line SCADA functions.

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

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

All newly defined points shall be initially presented to the user with default values for all parameters and characteristics where defaults are meaningful. It shall also be possible to 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.

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

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

4.6.1 Run-Time Database Generation and Maintenance

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

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

4.6.1.1 Data Retention

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

4.6.1.2 Making Database Online

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

Newly generated run-time databases shall only be placed on-line by user command. Following the assignment of a new database to a server and on user demand, the database management software shall access each SCADA server to ensure that all databases are consistent. Inconsistencies shall be annunciated to the user.

4.6.1.3 On-Line Database Editing

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

4.6.1.4 Tracking Database Changes

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

4.6.1.5 Initial Database Generation

The initial database shall contain all data required by the SCADA systems. Default values shall be used in consultation with NEA.

4.7 Display Generation and Management

SCADA displays shall be generated and edited using interactive display generation software delivered with the system. The display generator shall be available on development system & once the display/ displays creation/ modification activity is complete, the compiled runtime executable shall be downloaded on all workstations/servers.

The display editor shall support the important construction options like:-

- Copy/move/delete/modify,
- Building at different zoom level,

- Linking of any defined graphics symbol to any database point, Pop-up menus,

Protection of any data field on any display against user entry based on log-on 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 system shall be provided.

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

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

The display generation, compilation & loading shall not interfere with the online SCADA functions. All user interface features defined in this Specification shall be supported by the display generator.

4.7.1 Display Elements

The elements available to create a display shall consist of graphic primitives symbols, segments, User Interaction Field and layers. These elements shall be available to be linked to the SCADA functions and dynamically transformed on the display as governed by linkages to the database.

4.7.1.1 Segments

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

The display generator shall support the addition, deletion, and modification of segments,

including the merging of one segment with another to create a new segment. Segment size shall not be limited. Segments shall be defined at an arbitrary scale factor selected by the user.

4.7.1.2 Dynamic Transformation Linkages

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

4.7.2 Display Generation and Integration

The displays shall be constructed from the display elements described above. The display definition shall allow displays to be sized to meet the requirements of the SCADA application

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

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

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

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

4.8 Report Generation Software

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

The user shall be able to construct periodic reports and ad-hoc queries via interactive procedures. The capability to format reports for workstations and printers shall be provided. The user shall be able to specify the presentation format for periodic reports and ad-hoc query reports as alphanumeric display format, graphical display format, or alphanumeric printer format. The user shall be able to specify that processing functions, such as summations and other arithmetic functions, be applied to portions of the report data when the report is processed for display, printing, or file storage. The software shall provide for generation of reports that are the full character width of the printers and that use all of the printer's capabilities, such as font sizes and styles and print orientation. For report data editing, the user shall be able to obtain the data from a retained report, modify the data, repeat the inherent data calculations, reprint the report, and save it in a report retention file on auxiliary memory without destroying the original report.

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

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

4.9 System Generation and Build

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

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

4.10 Software Utilities

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

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

4.10.1 File Management NEA

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

4.10.2 Auxiliary Memory Backup NEA

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

(a) Server and workstation

(b) File names (including directory and wildcard designations)

(c) File creation or modification date and time

(d) Whether or not the file was modified since the last backup.

A backup NEA that can back up all server and workstation auxiliary memories on to a single target auxiliary memory or archive device shall be provided. The backup NEA must ensure that

the source auxiliary memory files are captured properly regardless of caching activity.

4.10.3 Failure Analysis NEA

Failure analysis NEA shall be provided to produce operating system and application program status data for analyzing the cause of a fatal program failure. The failure information shall be presented in a condensed, user-oriented format to help the user find the source of the failure. The information

shall be presented on displays and recorded for historical records and user- requested printed reports.

4.10.4 Diagnostic NEA

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

4.10.5 System utilization Monitoring NEA

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

4.10.6 Other NEA Services

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

------End of Chapter 4-----

CHAPTER -5: HARDWARE REQUIREMENTS FOR SCADA

5.0 Introduction

This chapter articulates the hardware requirements for the SCADA system. The bidders are encouraged to optimize the hardware for servers where SCADA & ISR applications can be combined or distributed in any combination with adequate redundancy. However, quantity of servers shall be as per detailed bill of quantities for SCADA defined in the BOQ. The bidder shall assess the adequacy of hardware specified in the BOQ & if any additional hardware is required to meet all the requirements of the technical specifications, the same shall also be included in the offer. The Bidder shall offer the minimum hardware configuration as specified here for various equipment, however if required, higher end hardware configurations shall be offered to meet all the requirements of the technical specification. The redundant hardware such as servers (Except DTS, development server) , CFE, etc. shall work in hot standby manner. It is necessary to ensure that the functional requirements, availability & performance aspects are met as per SCADA system specification.

5.1 General Requirements for Hardware

All hardware shall be manufactured, fabricated, assembled, finished, and documented with workmanship of the highest production quality and shall conform to all applicable quality control standards of the original manufacturer and the Contractor. All hardware components shall be new and suitable for the purposes specified. All hardware such as computers, computer peripherals/accessories etc. and networking products proposed and implemented shall conform to latest products based on industry standard. All hardware shall be of reputed make.

All servers and workstations shall include self-diagnostic features. On interruption of power, they shall resume operation when power is restored without corruption of any applications. The hardware shall be CE/FCC or equivalent international standard compliance. The specification contains minimum hardware requirement. However, the contractor shall provide hardware with configuration equal or above to meet the technical functional & performance requirement. Any hardware/software that is required to meet functional, performance & availability requirement shall be provided by Contractor & the same shall be mentioned in the BOQ at the time of bid . If not mentioned at the time of bid, contractor shall provide the same without any additional cost to the owner The proposed system shall be designed for an open & scalable configuration, to ensure the inter-compatibility with other systems of the NEA, the future smooth expansion as well as the easy maintainability. The proposed hardware configuration should be extended by adding either CPU processors / memory boards / disks etc.in delivered units or additional units for capacity extension.

The configuration of the SCADA shall comprise a distributed computing environment with an open systems architecture. The system architecture shall be open internally and externally to hardware or application software additions, whether supplied by the original supplier of the SCADA or obtained from third party vendors, both for capacity expansion and for upgrading functionality, without affecting existing SCADA components or operation.

All internal communications among the SCADA Servers and all external communications between the SCADA and other computer systems shall be based on widely accepted and published international or industry standards which are appropriate and relevant to the open systems concept

or should have a field proven acceptance. This applies to the operating system, database management system, and display management system, as well as to APIs providing standardized interfacing between System software and application software.

The contractor should ensure that at the time of final approval of hardware configuration/BOQ, all the above hardware are current industry standard models and that the equipment manufacturer has not established a date for termination of its production for said products. Any hardware changes proposed after contract agreement shall be subject to the following: -

a. Such changes/updates shall be proposed and approval obtained from NEA along with the approval of Drawings/documents.

b. The proposed equipment shall be equivalent or with better features than the equipment offered in the Contract.

c. Complete justification along with a comparative statement showing the original and the proposed hardware features/parameters including technical brochures hall be submitted to NEA for review and approval.

d. Changes/updates proposed will be at no additional cost to NEA.

5.2 Hardware Configuration

In this technical specification all hardware has been broadly classified as server and Peripheral device. The term "server" is defined as any general-purpose computing facility used for hosting SCADA & ISR application functions as defined in the specification. The servers typically serve as the centralized source of data, displays and reports. The term "Peripheral Device" is used for all equipment other than servers. Peripheral device includes Operator Workstations, WAN router, LAN, Printer, Time and Frequency system, External Auto loader, External Cartridge Magnetic tape drive, VPS, RTU etc.

Servers rack sizing SI with conduct a survey of DCC & DRC. Current rack sizing in DCC and DRC are 42U Server Racks (600 mm x 1200 mm) UL approved/complied.

5.2.1 Servers

The Server OEMs shall be members of TPC/SPEC. The servers are broadly classified into categories: Application (SCADA/ISR), Communication (FEP/ICCP), DMZ (Web), and Training/Development. The servers are broadly classified into the following categories:

A) Application server

- SCADA
- ISR
- NMS
- Web server

B) Communication server

- Front –End server (Communication Front End- FEP/CFE)

- ICCP /Inter control center communication server

C) De –militarized server (DMZ)

- Web server with load balancing

D) Training & development system server

- DTS
- Developmental server

E) Data recovery

- DRR/DR/ Communication server

Minimum Hardware Configuration: The servers shall be based on the latest generation Industry Standard Server Grade Architecture (x86-64 or equivalent high-performance RISC/ARMv8 architecture certified for the proposed SCADA application). The system must support open standard Operating Systems (Windows Server / Enterprise Linux)

- Processor: Latest generation Server Grade Processor. The processor performance shall meet a **SPECrate®2017_int_base score of minimum 150** (or equivalent industry standard published benchmark) to ensure high throughput and multi-processing capability.
- Memory: Minimum **64GB DDR4/DDR5 ECC Memory** (Scalable to at least 1TB). For Database/Historian/ISR servers, minimum **128GB** is required.
- Storage (Internal):
  - Boot/OS: Minimum 2 x 480GB Enterprise SSD/NVMe (Configured in RAID 1).
  - Data/Application: Minimum **4 TB Usable Capacity** using Enterprise Grade Hot-Pluggable SAS (10k RPM) or SSDs (Mixed Use) configured in RAID 5/6/10
- Network Interfaces:
  - 4 x 10/100/1000 Base-T (RJ45) Ports.
  - 2 x 10/25 Gbps SFP28 Ports (for High-Speed Storage/Backbone connectivity).
- Management: Integrated Intelligent Management Controller (e.g., iBMC, iDRAC, iLO, or equivalent) with dedicated 1Gbps management port, supporting remote KVM, Virtual Media, and predictive failure analysis.
- Peripheral Interfaces: Minimum 3 x USB 3.0 Ports (Front/Rear) for local high-speed data transfer.
- Optical Drive: Virtual Media support via Management Controller; Physical USB DVD-RW (Optional/External) if required for legacy media.
- Power Supply: Dual Redundant, Hot-Swappable Power Supply Units (PSU) rated for 230 VAC operation with Platinum/Titanium efficiency.
- Cooling: Redundant, Hot-Swappable High-Performance Fans.

- User Interface: 1 x 24-inch LED Professional Monitor, USB Keyboard, and Optical Mouse.

- Mounting & Access: The Contractor shall provide 19-inch Rack-Mounted servers with sliding rails. The Main & Standby servers shall be housed in separate panels/cubicles where applicable. Each server rack/cubicle shall be provided with a Foldable Rack-Mount KVM Console (Keyboard, Video, Mouse) with a 17-inch (or larger) LCD/LED display to manage multiple servers locally.

5.2.1.1 Application servers

Redundant SCADA servers shall house the SCADA application. Redundant ISR application servers shall be provided with a common external memory system for mass historical data storage and retrieval. The external memory shall comprise enterprise-grade hot-pluggable drives (SAS HDD or SSD) configured in a RAID architecture (RAID 5, 6, or 10) to ensure data redundancy and high availability.

The external memory shall be connected via high-speed iSCSI or Fibre Channel interfaces to ensure ample throughput for historical data recording and retrieval. Alternatively, the bidder may offer internal RAID storage with each server, provided it meets the mass storage and redundancy requirements.

Storage Array Specifications: The SCADA system shall include an Enterprise Unified Storage Array (SAN/NAS) configured to store historical data for the required retention period (7 Years) and sized for the Ultimate historical database capacity. The storage array shall meet the following minimum requirements:

- Storage Controllers: Dual-Redundant, Active-Active Controller architecture with automatic failover.

- Controller Cache: Minimum 32 GB per controller (Battery or Capacitor backed) to ensure write performance during power fluctuations.

- Host Interfaces: Minimum Dual 16 Gbps (or higher) Fibre Channel ports OR Dual 10/25 Gbps iSCSI ports per controller.

- Drive Support: The array shall support Enterprise Grade SAS (10k RPM) drives or Mixed-Use SSDs.

- RAID Levels: Supports RAID 1, 5, 6, and 10.

- Performance: The array shall be capable of delivering a minimum of 15,000 IOPS with sub-5ms latency to handle burst historical data writes.

- Usable Capacity: Minimum 20 TB Usable Capacity (calculated after RAID overhead and hot-spares).

Redundant Web / Active Directory Services Server shall host Web Applications for SCADA LAN and the DNS configuration. Redundant NMS server shall be provided to host NMS application

5.2.1.2 Communication Servers

5.2.1.2.1 FEP (CFE) Server

The redundant Front End Processor (FEP) server shall be a functional unit that offloads the task of communication and pre-processing between RTUs and SCADA servers. The FEP shall be based on the Server Hardware Specifications defined in Clause 5.2.1.

All RTUs shall be connected to the CFE through IEC 60870-5-104/101 links. The FEP shall support simultaneous communication on multiple protocols including IEC 101/104, DNP3, and Modbus. The system shall support multi-threading to manage high-density connections.

Scalability: The FEP architecture shall support horizontal scalability. It shall be possible to add additional FEP pairs to the LAN to handle network expansion without system shutdown.

Security: The CFE shall support Native SSL/TLS encryption and VPN tunneling for communicating with RTUs over public networks (GPRS/4G/5G). The FEP shall have Hardened OS compliance with no open ports other than those required for specific SCADA traffic. It shall support IPSec for secure data exchange. The equipment shall accept control commands only from designated Master IP addresses (Whitelisting).

Synchronization: The Communication Servers shall process time-stamped data and shall be synchronized via NTP/SNTP or PTP (Precision Time Protocol) from the GPS servers.

5.2.1.2.2 ICCP Server /inter control center communication server

The ICCP Server shall be based on the Server Hardware Specifications defined in Clause 5.2.1. Redundant ICCP servers shall be installed at the DCC and DRC/BCC to retrieve, transmit, and process data from remote sources (LDC/MCC) using IEC 60870-6 (TASE.2) or equivalent secure inter-control center protocols. The server shall support Secure ICCP (over SSL/TLS) as per IEC 62351 standards..

5.2.1.2.3 Network Management System (NMS) Servers

Redundant NMS servers shall be provided for configuration management, fault management, and performance monitoring of the IT/OT infrastructure.

Telemetry Support: The NMS shall support modern telemetry standards (e.g., SNMPv3, IPMI, and Flow-based monitoring like sFlow/NetStream/IPFIX) to provide real-time visibility into network traffic and micro-bursts.

Visual O&M: The system shall provide a graphical topology view and support AI-driven Fault Diagnosis to predict potential hardware failures.

5.2.1.2.4 Web servers with Load Balancing

The Web Servers shall be configured in a high-availability cluster (Active-Active) with a Hardware or Virtual Application Delivery Controller (Load Balancer).

Performance: The Load Balancing mechanism shall support a minimum of 1 Gbps Throughput and 5,000 SSL Transactions Per Second (TPS) to ensure secure HTTPS access for external users.

Security: The Web subsystem shall be isolated in a DMZ and protected by Host-based Intrusion Detection Systems (HIDS). It shall serve data via a Data Replica mechanism to ensure no direct external access to the SCADA Real-Time Database.

5.2.1.2.4 Active Directory Server (AD Server)

The authentication of the users for the all systems will be done via Active Directory(AD) servers. All users and computers in a Windows domain network will be authenticated through AD servers. Assigning and enforcing security policies for all computers in a Windows domain network. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal

user. Active Directory makes use of Lightweight Directory Access Protocol (LDAP), Kerberos and DNS.

The supplier shall stipulate that their provided system is compatible with Microsoft Active Directory (AD) based on the latest Windows Server operating system, in order to coordinate user definitions within the Operations Network. The supplier must also supply any information regarding additional AD plug-ins, which would be required to interface between the system and AD server.

5.2.1.3 Demilitarized/ Security servers

5.2.1.3.1 Web servers with Firewalls

Redundant Firewall & IPS Specifications: The Security System shall employ Next-Generation Firewalls (NGFW) in High Availability (HA) mode.

- Architecture: Dedicated Security Appliance (Hardware or Carrier-Grade Virtual Appliance) with Hardware Acceleration for encryption offloading.
- Performance:
  - Threat Protection Throughput: Minimum 1 Gbps (with Firewall + IPS + Antivirus + Application Control enabled).
  - FW Throughput: Minimum 5 Gbps.
  - Concurrent Sessions: Minimum 100,000.
- Features: The firewall shall support AI/Machine Learning-based Unknown Threat Detection, Deep Packet Inspection (DPI) for SCADA protocols (IEC 104, DNP3, Modbus), and SSL Inspection.
- Encryption: Support for AES-256, SHA-2, and IKEv2.
- Certifications: The technology shall be certified by independent global bodies (e.g., ICSA Labs, EAL4+, or NSS Labs recommended rating) to ensure audit compliance.

5.2.1.4 Training & development system server

5.2.1.4.1 DTS server

A non - redundant server to host DTS applications shall be provided to impart the training.

5.2.1.4.2 Development server

A non- redundant server to host Developmental applications shall be provided

5.2.1.5 5.2.1.5 Data recovery

The Data Recovery and ISR Systems shall be supported by an Enterprise Unified Storage Array (SAN/NAS).

- Controllers: Dual-Redundant, Active-Active Controller architecture.
- Cache: Minimum 32 GB per controller (Battery/Capacitor backed).
- Interfaces: Minimum 4 x 16 Gbps Fibre Channel OR 4 x 10/25 Gbps iSCSI ports.
- Capacity: Minimum 20 TB Usable Capacity (calculated after RAID overhead).
- Performance: Minimum 15,000 IOPS at sub-5ms latency.
- Reliability: The system shall support RAID 6 or RAID-TP (Triple Parity) for high fault

tolerance.

- Intelligence: The storage shall feature AI-Driven Operations (AIOps) for intelligent capacity planning and failure prediction.

5.2.2 Operator Workstations

The operator Workstation console shall be used as a Man Machine Interface (MMI) by despatcher for interacting with all SCADA system. Operator Workstation consoles shall also be used as development console to take up developmental/ maintenance activities such as generation/updation of database, displays etc.& to impart training through DTS workstation consoles.Each workstation shall consist dual monitors & single keyboard and a cursor positioning device/mouse.

Workstation consoles for development system shall also be available with single TFT monitor Operator workstation consists of a console driving single/ dual monitors as defined in the BOQ. The user shall be able to switch the keyboard and cursor-positioning device as a unit between both monitors of console. The minimum hardware configuration of operator workstation shall be:

- Workstations shall be Professional Grade Workstation PCs (e.g., Dell Precision, HP Z-Series, Lenovo ThinkStation, or equivalent).
- Memory: Minimum 32 GB DDR4/DDR5 RAM.
- Storage: Minimum 512 GB NVMe SSD (Class 40/50).
- Graphics: Dedicated Professional Graphics Card (NVIDIA RTX / AMD Radeon Pro) with minimum 4 GB GDDR6 memory, capable of driving dual/triple 4K displays.
- Monitors: Dual 24-inch Professional IPS LED Monitors (FHD or higher, Anti-Glare, DisplayPort/HDMI).
- Peripherals: USB Keyboard, Optical Mouse, and Multimedia Speakers.
- Dual 10/100/1000Mbps Ethernet ports

The specification of Remote VDU is same as of workstation for SCADA system mentioned above, except, it shall have suitable software & hardware to facilitate remote VDU user to monitor remotely, the real time power system from SCADA system & have facility to generate report. The additional associated hardware is mentioned in the BOQ.

5.2.4 WAN router

The WAN Router shall be an Industrial Services Router designed for mission-critical SCADA data exchange between Control Centers, Remote VDUs, and Substations over MPLS/OTN/GPRS networks. The router shall support modular architecture to accommodate various connectivity interfaces (Fiber, Copper, Cellular).Working on G.703 interface & OSI and TCP/IP protocols

- Architecture & Performance:
    - Forwarding Performance: Minimum 100 kpps (Kilo Packets Per Second) for 64-byte packets to ensure handling of high-density SCADA telemetry.
    - Encrypted Throughput: **Encrypted Throughput: Minimum 1 Gbps** (to handle aggregation of 215 remote sites).
    - Availability: The router shall support Virtual Router Redundancy Protocol (VRRP) or equivalent open standard for High Availability (HA) failover.

- Operating Environment: Industrial grade design suitable for substation environments (-10°C to +60°C).

- Interfaces:
  - **LAN/WAN Ports:** Minimum 2 x Gigabit Ethernet Combo Ports (RJ45/SFP) for uplinks and 2 x Gigabit Ethernet LAN ports.
  - **Cellular Connectivity:** Built-in or Modular slot for **4G LTE / 5G** Modem with Dual-SIM support for carrier redundancy.
  - **Legacy Support:** If required for specific sites, the router shall support optional Serial RS-232/RS-485 modules (user configurable).
- Protocols & Routing:
  - **Routing:** Support for Open Standards including IPv4/IPv6, **OSPFv2/v3, BGP, IS-IS**, and Static Routing.
  - **VPN & Security:** Support for IPsec (Site-to-Site), GRE, SSL VPN, and **DMVPN** (or equivalent scalable VPN technology). Encryption support for AES-256 and SHA-2.
  - **QoS:** Advanced Quality of Service (QoS) including Low Latency Queuing (LLQ), Class-Based Weighted Fair Queuing (CBWFQ), and Traffic Shaping/Policing to prioritize SCADA traffic over management traffic.
- Management & Telemetry:
  - **Management:** Console port (USB/Serial), SSHv2, HTTPS, and SNMPv3
  - **Telemetry:** Support for **Network Flow Monitoring** (e.g., NetFlow, sFlow, IPFIX, or NetStream) for real-time traffic analysis and micro-burst detection.
  - **Zero-Touch Deployment:** Support for secure zero-touch provisioning to simplify remote installation.

The data exchange between the two centers shall be primarily over MPLS based secured network using TCP/IP on various mediums as per the requirement and availability in the respective project area viz FO, radio, V-SAT etc.by network bandwidth service provider (NBSP) part of SI team. The router shall support the OSI and TCP/IP protocols.

The Wide Area Links are planned for 2Mbps or higher Bandwidth capacity from ISPs. The Router offered shall deliver high performance IP/MPLS features and shall support Layer 3 MPLS VPN connection. It shall support PPP/Frame Relay transport over MPLS.

The Routers shall be configurable and manageable through local console port, http interface, NMS software and as well through Telnet.

The Router shall provide built-in monitoring and diagnostics to detect failure of hardware. The Router shall be provided with LED/LCD indication for monitoring the Operational status. The configuration changes on the Router should take effect without rebooting the router or modules.

1. **Memory Flash:** Minimum *2GB*
2. **Console Port:** 01 No. for configurations and diagnostic tests
3. **LAN/WAN Port:** The router shall use G.703 E1 & high speed Ethernet and provide support variety of interfaces as per the concerned NEA's requirement at site like V.24/V.35, E1, Channelized E1 etc. along with following minimum number of

ports:

- Two fixed 10/100Mbps high speed Ethernet ports
- Additionally, if contractor also needs Serial ports with synchronous speed up to 2 Mbps to meet functional and performance requirement in addition to ethernet ports and if need be for functional/performance requirement then interface shall serial port for V.35/V.24/ x.21 to be considered
- SIM Slot with 3G/4G or higher connectivity
- Two fixed ports of G.703 E1 (2 Mbps) interface & One AUX port

Total no of ports shall be determined by the connectivity requirement.

All the interface cables for interconnecting all LAN/WAN ports as well as connection to SCPC/MCPC/ leased E1 – V.35 ports etc. shall be in the scope of bidder.

The device shall have MAC addressing filtering per port.

4. **Scalability**: Should have provision of at least 100% additional number of free ports for future scalability
5. **Network Protocol:** TCP/IP and support for IP version 6. Shall provide IP address management
6. **Routing Protocols:**

RIP v1 (RFC 1058), RIPv2 (RFC 1722 AND 1723), OSPFv2 (RFC1583 & RFC 2328), OSPF on demand (RFC 1793), BGP4 with CIDR implementation as per RFC 1771. The implement should be compliant as per RFC1745 that describes BGP4/IDRP IP OSPF interaction. It shall provide Policy routing to enable changes to

normal routing based on characteristics of Network traffic. IS-IS protocol support (RFC 1195).

7. **WAN Protocols:**

Frame Relay(LMI & Annexed & ITU Annex A), PPP (RFC1661), Multi-link PPP (RFC1717), HDLC/LAPB, Frame Relay support shall include multi-protocol encapsulation over Frame relay based on RFC1490, RFC 1293 for Inverse ARP/IP,DE bit support. Support of protocols of VPNL, L2TP,L2VPN, L3VPNs

8. **High Availability:**

Shall support redundant connection to LAN For high availability, the router should support the standards-based RFC 2338 Virtual Router redundancy Protocol (VRRP) or equivalent

9. **Network Management:**

SNMP, SNMPv2 support with MIB-II and SNMP v3 with Security authentication. Implementation control configuration on the Router to ensure SNMP access only to SNMP Manager or the NMS workstation.

- RMON 1 & 2 support using service modules for Events, Alarms, History.
- Should have accounting facility.

- Shall support multilevel access.
- Shall be Manageable from any Open NMS platform.
- Shall support for telnet, ftp, tftp and http & https enabled Management.
- Should have debugging facility through console.
- AAA Authentication support shall be provided via RADIUS (Remote Authentication Dial-IN User Service) and/or TACACS, PAP/CHAP authentication for P-to-P links, 3DES/IPsec encryption with hardware-based encryption services.

10. Optimization feature:

Data Compression for both header and payload to be supported for Frame Relay and Leased/Dial-up WAN Links. Dial restoral on lease link failure Dial on demand or congestion, Load Balancing.

Support for S/W downloads and quick boot from onboard Flash. Online software re-configuration to implement changes without rebooting. Should support Network Time Protocol for easy and fast synchronization of all Routers.

11. QOS Support:

RSVP (Resource Reservation Protocol as per RFC 2205), IGMP v1, v2 (Inter Group Management Protocol Version 2 as per RFC 2236), Multicast Routing support like PIM-SM (RFC 2362), PIM-DM etc.

Policy based routing (It shall be possible to affect the normal routing process for specific mission critical traffic through specified alternate routes in the network). A class based scheduling, Priority Queuing mechanism that shall provide

configurable minimum Bandwidth allocation to each class and IP Precedence. Congestion Avoidance –Random Early Detection (RED). Support for Differentiated Services as per RFCs 2474, 2475, 2598 & 2597.

5.2.5 Local Area Network (LAN) and Device Interfaces

Servers, consoles, and devices are connected to each other on a local area network (LAN), which allows sharing of resources without requiring any physical disconnections and reconnections of communication cables.

LAN shall have the following characteristics:

A. **Network Architecture** Four distinct LAN segments shall be formed: SCADA, DTS, Development System, and DMZ.

- **Dual (Redundant) LAN:** Envisaged for the SCADA system and DMZ system to ensure high availability. The Backup Control Center (BCC) shall also use redundant LAN.
- **Single LAN:** Envisaged for the DTS and Development system

B. **Functional Requirements** The LAN shall have the following characteristics:

- Shall conform to the ISO 8802 or IEEE 802 series standards.
- Shall preclude total LAN failure if a single server, device, or their LAN interface fails.

- Shall allow reconfiguration of the LAN and the attached devices without disrupting operations.

C. **LAN Switch Hardware Specifications** The LAN Switches shall be **Enterprise Grade Managed L2/L3 Switches** complying with the following technical parameters:

- **Port Density:** 24 or 48 Ports 10/100/1000 Base-T (as per specific BOQ location requirement).
- **Uplinks:** Minimum 4 x 1/10 Gbps SFP+ uplinks per switch.
- **Performance:** Non-blocking switching fabric with minimum 128 Gbps capacity.
- **Features:** VLAN (802.1Q), QoS, Link Aggregation (LACP), MAC Security, and Network Telemetry.
- **Efficiency:** IEEE 802.3az Energy Efficient Ethernet compliance.

5.2.6 Printers

Except for the output capabilities unique to any printer type (such as extended character sets, graphic print and coloring features), there shall be no limitations on the use of any printer to perform the functions of any other printer. All the SCADA system printers shall have a standard 10/100/1000 Mbps Ethernet (RJ45) interface. The characteristics for each type of printer are described below:

A. Black & White Laser Printer

It is a multipurpose printer used to take prints of displays, reports etc. The laser printer shall have the following features:

- Shall be black & white laser printer
- Minimum speed 40 ppm
- Resolution 1200 x 1200 dpi
- Network Ready (Gigabit Ethernet)
- Duplexing (Automatic 2-sided printing)
- Landscape and portrait output orientation
- Memory buffer of at least 512 MB
- Shall be suitable for A4/Letter size normal paper

B. Colour Laser Printer

It is a multipurpose printer used to take prints of displays, reports etc . The color laser printer shall have the following features:

- Shall be color laser printer
- Minimum speed 30 ppm
- Resolution 1200 x 1200 dpi
- Network Ready (Gigabit Ethernet)

- Minimum 1 GB Memory
- Landscape and portrait output orientation
- Duplex printing (Automatic 2-sided printing)
- Shall be suitable for A4/Letter size normal paper

5.2.7 Time and Frequency system

GPS based time facility, using Universal Time Coordination (UTC) source, shall be provided for time synchronization of computer system at SCADA control center. The time receiver shall include an offset adjustment to get the local time. It shall have propagation delay compensation to provide an overall accuracy of ±1.5microsec. The GPS system shall have dual 10/100/1000Mbps LAN interface. The GPS receiver shall be provided in redundant configuration.

The time receiver shall detect the loss of signal from the UTC source, which shall be suitably indicated. Upon loss of signal, the time facility shall revert to its internal time base. The internal time base shall have a stability of 2pm or better.

The GPS system shall include digital displays for time and date in the format DDD:HH:MM:SS (the hour display shall be in 00 to 23 hour format)

GPS system shall also be used to drive separate time, day & date indicators which shall be wall mounted type. The display for time shall be in the 24-hour, HH:MM:SS format. The display for the day & date shall be xxx format (MON through SUN) & DD:MM:YYYY respectively. Contractor shall provide wall mounted type digital display units for time, day, date & frequency indication. The display of frequency shall be in the xx.xx Hz format. The frequency shall be derived from 230V AC supply.

Each digit on the time, day and frequency indicators shall be at least 7.5 cm in height and shall be bright enough for adequate visibility in the control room from a distance of 15 meters. The offered GPS clock shall also provide at least one 2 MHz (75 ohm interface confirming to ITU-T G.703) synchronization interface to meet the time synchronization requirement of the communication system. This interface shall confirm to the requirements specified in ITU-T G.811 for accuracy, jitter, wander etc. Alternatively, a separate GPS clock for synchronization of communication system is also acceptable.

5.2.8 Furniture

NEA shall provide necessary furniture & shall look aesthetically pleasing. It is not in the scope of contractor.

5.3 Auxiliary Power Supply for Computer systems

The computer system should be suitable for operation with single-phase, 230 ±10% Vac,50 ±5.0% Hz power supply. To ensure uninterrupted & regulated power supply to computer system, suitable rating UPS are envisaged under auxiliary power supply specification. All cables supply, laying & their termination between UPS panel & computer system shall be in the scope of contractor.

The input circuit breakers are provided in the UPS for protection against short circuits, any additional fuses, switches and surge protection if necessary to protect the hardware shall also be supplied by the Contractor.

The auxiliary power to all computer system hardware shall be fed from parallel operating UPS

system. On interruption of input AC power to UPS, the load shall be fed through UPS inverter through its batteries. In case of battery capacity low conditions (due to prolonged failure of input supply to UPS), the computer system shall go for orderly shutdown to avoid corruption of any applications. The orderly shutdown of computer system can be implemented either through RTU (where UPS alarms shall be wired to RTU) or through suitable interface with UPS Supplier software.

5.4 Environmental Conditions

Equipment to be located in the SCADA control center building shall operate over an ambient temperature range of 16 C to 32 C, with a maximum rate of change of 5 C per hour. Relative humidity will be less than 80% non-condensing. In case of Altitude of 2000MSL or more, the same may be specified by NEA.

5.5 Acoustic Noise Level

The noise level of any equipment located in the control room shall not exceed 60dbA measured at three feet from equipment especially for the printers.

5.6 Construction Requirements of panels

In case the equipments are mounted in panel type of enclosures, then such enclosures shall meet the following requirements:

a. shall be free-standing, floor mounted and shall not exceed 2200 mm in height.

b. Enclosures shall be floor mounted with front and rear access to hardware and wiring through lockable doors.

c. Cable entry shall be through the bottom. No cables shall be visible, all cables shall be properly clamped, and all entries shall be properly sealed to prevent access by rodents.

d. The safety ground shall be isolated from the signal ground and shall be connected to the ground network Each ground shall be a copper bus bar. The grounding of the panels to the owner's grounding network shall be done by the contractor.

e. All enclosures shall be provided with, 230 VAC 15/5A duplex type power socket & switch for maintenance purpose.

f. All panels shall be provided with an internal maintenance lamp and space heaters, gaskets.

g. All panels shall be indoor, dust-proof with rodent protection, and meet IP41class of protection.

h. There shall be no sharp corners or edges. All edges shall be rounded to prevent injury.

i. Document Holder shall be provided inside the cabinet to keep test report, drawing, maintenance register etc.

j. Cooling air shall be drawn from the available air within the room.

k. 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.

l. Suitable sized terminal blocks shall be provided for all external cablings.

5.7 Assembly and Component Identification

Each assembly in the system, to the level of printed circuit cards, shall be clearly marked with the manufacturer's part number, serial number, and the revision level. Changes to assemblies shall be indicated by an unambiguous change to the marked revision level. All printed circuit card cages and all slots within the cages shall be clearly labelled. Printed circuit cards shall be keyed for proper insertion orientation.

5.8 Interconnections

The Contractor shall supply all signal cabling for computer system components, using polarized plug-type connectors to ensure proper assembly. Each cable shall be continuous, without intermediate splices, and clearly marked at both ends with its number and termination details. All terminations shall be within enclosures.

Similarly, the Contractor shall supply and install RTU cabling, including connections to the interface cabinet, MFTs/MFMs, and relay panels in the substation control room, ensuring accurate representation in contractor-supplied drawings. Internal interconnections shall use plug-type or compression connectors with proper polarization. Adequate space and necessary hardware shall be provided within enclosures for field wiring, which shall be neatly arranged and not directly fastened to the enclosure frame. Internal wiring and cables shall be routed separately from field wiring to RTU terminals and power wiring. All wiring shall use flame-retardant copper conductors, with multi-conductor cables individually color-coded. The use of non-flammable, self-extinguishing plastic wire troughs is allowed, while metal clamps, if used, must have insulating inserts. Wiring between stationary and movable components, such as across door hinges or on extension slides, shall allow full movement without binding.

5.9 Consumables

The Contractor shall supply, at its own expense, all consumables required for use during all phases of the project through completion of the system availability test. The consumable items shall include as minimum :

(a) Printer paper

(b) Printer toner, ink. Ribbons and cartridges

(c) storage devices like Blu-ray disc /CD in line with storage device of Server or Workstation

-----End of Chapter 5-----

CHAPTER 6: CONFIGURATION & SYSTEM AVAILABILITY

6.0 General

This chapter describes the requirement of monitoring and managing the SCADA system with regard to its configuration and availability under normal conditions and under hardware and software failure conditions.

6.1 System Redundancy

The system envisages some functions as critical functions and others as non-critical functions. The critical functions shall have sufficient hardware and software redundancy to take care of hardware or software failure condition whereas non-critical functions may not be provided with hardware and software redundancy. The redundancy requirement for hardware of SCADA system shall be as follows:

(a) Servers: The servers for , ICCP, Communication servers, ISR application, servers for DMZ/ security system systems, DR and shall be configured as redundant system. (Except for DTS , development server)

(b) LAN and device interface: LAN shall be configured as redundant. All equipment, except DTS, development system shall have single LAN)

(c) Printers: All Printers shall be non- redundant devices.

(d) Operator workstations/ Remote VDUs: These shall be configured as non-redundant devices.

(e) Time and frequency system: The GPS receiver of time and frequency system shall be configured as a redundant device at SCADA control center.

(f) Communication front end (CFE): Communication front end shall be configured as redundant system.

(g) WAN Router: The WAN router connected to dual LAN shall have channel redundancy.

Every critical function must be supported by sufficient hardware redundancy to ensure that no single hardware failure will interrupt the availability of the functions for a period exceeding the automatic transfer time.

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.

6.2 Server and Peripheral Device States

Server and peripheral device states represent the operating condition, of each server and peripheral device. The various states have been defined below: The system's reaction to restart/failover operations shall be governed by the state. Server and peripheral device states shall be assigned by the function restart, server and device failover functions, and by user command.

6.3 Server States

Each server shall be assigned to one of the following states:

(a) Primary State: In primary state, a server performs any or all of the on-line functions described in this specification and is referred as primary server. A primary server shall concurrently perform maintenance functions (e.g. update of database,

display and reports).

(b) Backup State: A server in backup state is referred as backup server. A backup server replaces a primary server/primary server group in the event of primary server/primary server group failure or upon user command. It shall communicate with the primary server(s) to maintain backup databases and monitor the state of the primary server(s). A backup server shall concurrently perform maintenance functions.

(c) Down State: A server in down state shall not communicate with the computer system and is not capable of participating in any system activity

6.4 Peripheral Device States

Each peripheral device shall be assigned to one of the following states:

(a) Primary state: A device in primary state is referred as primary device. The primary 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 device shall follow the reassigned functions.

(b) Backup state: A device in backup state is referred as backup device. A backup device is used to replace a primary device in the event of primary device failure. It shall communicate with the primary server or primary server group to inform its readiness for its assignment as a primary device. A device may be assigned to the backup state by the server function and by user action.

A backup device may participate in on-line activity along with the primary device as can be the case with LAN s. For such cases, failure of any one device shall cause other device to take up the role of both devices.

(c) Down state: A device in down state is referred as down device.

A down device cannot be accessed by the computer system.

6.5 Functional Redundancy

Every critical function must be supported by sufficient hardware redundancy to ensure that no single hardware failure will interrupt the availability of the functions for a period exceeding the automatic transfer time.

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.

6.6 Backup Databases

Copies of all databases shall be maintained on the Backup server so that system operations may continue in the event of Primary server, peripheral 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 60 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

d) 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)

e) Changes resulting from the addition or deletion of items and restructuring of databases in an existing database shall be automatically accommodated in the backup database.

6.7 Error Detection and Failure Determination

All servers, peripheral devices, on-line software functions, and maintenance functions in SCADA system shall be monitored for fatal error and recoverable errors. All errors shall be recorded for review by maintenance personnel. Each type of error (e.g., server failure, memory access violation, device reply to time-out, or message checksum error) shall be recorded separately with a date and time tag.

6.8 Server and peripheral device Errors

The Server/Device shall be declared as failed in case of fatal error. Server and peripheral device failure shall be detected and annunciated to the user within 10 seconds of the failure. For each type of recoverable error the programmer shall assign a threshold. When the count of consecutive recoverable errors exceeds this threshold, a warning message shall be issued to the operator.

6.9 Software Errors

Execution errors in on-line and maintenance functions that are not resolved by program logic internal to the function shall be considered fatal software errors. Examples of errors that may be resolved by internal program logic include failure of a study function to achieve a solution due to violation of an iteration limit or arithmetic errors (such as division by zero) which are caused by inconsistent input parameters or data. These errors shall produce an alarm informing the user of the error but shall not be considered 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 on-line function and each maintenance 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.

6.10 Server Redundancy and Configuration Management

Each server or server group supporting the CRITICAL functions described in the specifications, shall include at least one redundant server. The redundant server shall normally be assigned

to the backup state and shall take the role of a primary server in the event of failure or upon user command.

When a failure of a primary server in a redundant group is detected, the SCADA computer system shall invoke the appropriate failover and restart actions so that on- line functions assigned to the failed server are preserved. The on-line functions of the failed primary server shall be assigned

to the backup server by execution of a function restart within 30 seconds after detection of server failure, except for ISR function. For ISR server function the corresponding time shall be within 120 seconds after detection of server failure in case of failure of ISR sever, the ISR data shall be stored in the SCADA system till the failover of ISR server is completed to avoid data loss. This stored data shall be transferred to the ISR server automatically after restoration of ISR server.

If on-line functions are restarted in a backup server, the server's state shall be changed to primary. If backup servers are not available to perform the required functions, the SCADA computer system shall attempt to restart the failed primary server. A complete restart of the System, including full update from the field, shall not more than the stipulated time as specified above. No data shall be lost during the transfer of operation.

A failover (transfer of critical functions) to an alternate Server shall occur, as a minimum, under any one of the following situations:

- Non-recoverable failure of a server performing a critical function
- User request for a transfer of servers
- Failure of a periodic / scheduled function to execute on schedule.
- Violation of a configurable hardware device error counter threshold.

Failure of non-critical function shall not cause server failover. Functions assigned to a failed server in a non-redundant group may be lost until the failed server is restored to service. Failure of server operating in the backup state shall not initiate failover action.

Failed server shall be switched from down to any other state by user command only. All server reinstatement actions shall result in operator message. The messages shall identify the server(s) affected, all server state changes, and the success or failure of any restart operations.

6.11 Server Startup

Server startup shall be performed when commanded by a user, 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 SCADA computer system LAN. Subsequent to server startup, a function restart shall bring the server(s)to the appropriate server state.

Server Startup requirements are as follows:

Cold Start: In which default values are used for entire database. A cold start would be used only to build the initial SCADA and to recover from extraordinary failure conditions. Server startup shall be completed within 15 minutes and all applications shall be operational within 20 minutes of applying power except for ISR server and its database initialization, which can be up to 60 minutes.

Warm Start: In which a previously saved version of the database shall be used to initialize all real time data values. Server startup shall be completed within 10 minutes and all applications shall be operational within 15 minutes of application of power.

Hot Start: In which the memory resident version of database shall be used for continued operation. No reload of saved data shall be performed, although application software restarts. The intent is that after hot restart, only the operations being performed at the time of failure may be

lost. All online applications shall be operational not more than failover time.

6.12 Peripheral Device Redundancy and Configuration Management

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. All device failures shall be annunciated by alarms.

6.13 System Configuration Monitoring and Control

Required displays shall be provided for the user to review the system configuration and to control the state of the equipment. The following operations shall be possible:

- Fail-over, switching of states and monitoring of Servers and peripheral devices.
- Control of the resource usage monitoring function and display of server resource utilization
- The user shall be provided with the capability to interact with all functions using displays.

  It shall be possible to atleast Stop, Start, inhibit /enable and Restart any of the functions.
- Displays to view and control the status of backup databases shall also be provided.

-----End of Chapter 6------

CHAPTER 7: TESTING & DOCUMENTATION

7.0 General

This chapter describes the specific requirements for testing and documentation of the SCADA system.

7.1 Type testing

Equipment wherever mentioned in the specification for type testing shall conform to the type tests listed in the relevant chapters. Type test reports of tests conducted in National accredited Labs or internationally accredited labs with in last five years/ or validity of test of certificate whichever is lower from the date of bid opening may be submitted. In case, the submitted reports are not as per specification, the type tests shall be conducted without any cost implication to NEA before approval during design & engineering. If there is a difference between the type test requirement mentioned above specification and type test requirement mentioned in the respective sections.

7.2 Ad –doc testing

NEA may optionally ask SI to stage ad-doc testing in presence of team comprising of ADB, NEA. Other members may also be opted like, by like , Nodal agency . for basic of prototype of SCADA functions of offered product with simulated offered at least 2 RTU and balance by simulation for one sample project area . The same may be considered in design & engineering stage

7.3 Factory Acceptance Tests (FAT)

For each substation SCADA system including backup control center (BCC is part of the project area) shall be tested at the Contractor's facility. All hardware and software associated with the SCADA system and atleast two RTUs along with, LDMS, & all Remote VDUs, shall be staged for the factory testing and all remaining RTUs shall be simulated for the complete point counts (ultimate size).

Each of the factory tests described below (i.e. the hardware integration test, the functional performance test, integrated system test and unstructured tests) shall be carried out under factory test for the SCADA system. The factory tests, requiring site environment, shall be carried out during the Field Tests after mutual agreement for the same from owner.

7.3.1 Hardware Integration Test

The hardware integration test shall be performed to ensure that the offered computer hardware, conforms to this Specification requirements and the Contractor- supplied hardware documentation. All the SCADA system hardware shall be integrated and staged for testing. Applicable hardware diagnostics shall be used to verify the hardware configuration of each

equipment. The complete hardware & software bill of quantity including software licenses & deliverables on electronic media shall also be verified

7.3.2 System Build test

After completion of hardware integration test, the system shall be built from the backup software incl one copy of backup software on electronic media (CDs/ Tapes) to check the completeness of backup media for restoration of system in case of its crashing/failure

7.3.3 Functional Performance Test

The functional performance test shall verify all features of the SCADA hardware and software. As a minimum, the following tests shall be included in the functional performance test:

a) Testing of the proper functioning of all SACADA & other software application in line with the requirements of various sections of technical specification.

b) Simulation of field inputs (through RTU) from test panels that allow sample inputs to be varied over the entire input range

c) Simulation of field input error and failure conditions

d) Simulation of all type of sample control outputs

e) Verification of RTU communication Protocol IEC-60870-5-104 /101 etc

f) Verification of MFT communication Protocol MODBUS etc

g) Verification of compliance of supporting interfaces such as IEC61850, IEC60870-5-103 etc.

h) Verification of Security & Encryption using SSL for all RTU Connectivity.

i) All the hardware should be cyber security compliant.

j) Verification of data exchange with other systems

k) Verification of interoperability profile of all profiles of all protocols being used.

l) Verification of RTU communication interfaces

m) Verification of LAN and WAN interfaces with other computer systems

n) Testing of all user interface functions, including random tests to verify correct database linkages

o) Simulation of hardware failures and input power failures to verify the reaction of the system to processor and device failure

p) Demonstration of all features of the database, display, and report generation and all other software maintenance features on both the primary and backup servers. Online database editing shall also be tested on primary server.

q) Demonstration of the software utilities, libraries, and development tools.

r) Verification that the SCADA computer system meets or exceeds NEA's performance

s) Verification that ultimate expansion requirements are met.

t) Verification of DTS system

u) Verification of data transfer of main to back up SCADA system. (s) Functions of DR (DRC) system, if it is in the project area.

v) Unstructured testing of the SCADA system by NEA. The unstructured tests shall include the test, which are not in the approved test procedures and may be required to verify the compliance to the specification.(Max 20% of total testing)

7.3.4 Continuous operation Test (48 hours)

This test shall verify the stability of the hardware and software after the functional performance test has been successfully completed. During the test, all SCADA functions shall run concurrently and all Contractor supplied equipment shall operate for a continuous 48 (forty eight) hour period with simulated exchange with other interconnected system IT system envisaged etc. The test procedure shall include periodic repetitions of the normal and peak loading scenarios defined**.** These activities

to be tested may include, but shall not be limited to, database, display, and report modifications, configuration changes (including user-commanded processor and device failover), switching off of a primary server and the execution of any function described in this Specification. During the tests, uncommanded functional restarts or server/device failovers are not allowed; in case the problems are observed, the Contractor shall rectify the problem and repeat the test.

7.4 Field Tests (Site Acceptance tests -SAT)

The SCADA system shall be tested at the site. All hardware and software associated with the SCADA system along with all RTUs along with all field devices including MFTs connected shall be tested under the field tests.

7.4.1 Field Installation Tests

The equipment which has undergone the factory testing shall be installed at site and integrated with the RTUs and other computer systems though the communication medium.

The field installation test shall include the following:

(a) Proper installation of all delivered hardware as per approved layout.

(b) Interconnection of all hardware

(c) Interconnection with communication equipment

(d) Interconnection with power supply

(e) Diagnostic tests to verify the operation of all hardware

The Contractor shall be responsible for performing the field installation tests and NEA may witness these tests

7.4.2 End-to-End Test

After the field installation tests, the Contractor shall carry out end-to-end test to verify:

a) the RTU communication channel monitoring in the SCADA system

b) the mapping of SCADA database with RTU database for all RTU points

c) the mapping of SCADA database with displays and reports

The Contractor shall provide the details of all the variances observed and corrections carried out during end-to-end test.

7.4.3 Field Performance Test

The field performance test shall concentrate on areas of operations that were simulated or only partially tested in the factory (e.g., system timing and loading while communicating with a full complement of RTUs and data links and system reaction to actual field measurements and field conditions). Further the validity of factory test results determined by calculation or extrapolation shall be examined.

After the end-to-end test, the Contractor shall conduct the field performance test to verify the functional performance of the system in line with the technical specification which includes the following:

a) The communication of other system envisaged, if any e.g. IT , LDC, DR system

b) Verify that all the variances observed during the Factory test are fixed and implemented.

c) Conduction of the Factory tests deferred (tests requiring site environment)

d) Functional tests of SCADA system

e) Verify update rate & time for data update & control command execution as per specification requirements

f) Verify the response time for User interface requirements

g) Testing of all features of the database, display, and report generation and all other software maintenance features on both the primary and backup servers. Online database editing shall also be tested on primary server.

h) Conduction of unstructured tests as decided by NEA

7.4.4 Cyber security compliance

Compliance of cyber security without threatening vulnerabilities by IT Security Certification empaneled agency of GoN before Operational acceptance by SI shall be carried out.

7.5 System Availability Test (360 hours) - SAVT

Contractor shall provide & approve theoretical and practical figures used for this calculation at the time of detailed engineering. The calculation shall entail reliability of each individual unit of the System in terms of Mean Time between Failures (MTBF) and a Mean time to Repair (MTTR) as stated by OEM. Reliability figures of existing equipment shall be supported by evidence from operational experience at similar types of installation / figure given by OEM.

From those data, the unavailability of each sub-system shall be calculated taking in account each item redundancy. The global availability shall then be calculated from those different unavailability data. This calculation shall lead to the failure probability and equivalent global MTBF data for the control center system.

The overall assessment of System availability shall be provided in the form of an overall System block diagram with each main item shown, complete with its reliability data. The calculation of overall availability shall be provided with this diagram.

System availability tests shall be conducted after completion of the field tests. The system availability test shall apply to the system hardware and software integrated with its RTUs and legacy system envisaged However, the non- availability of RTUs/Data Concentrators , legacy IT system etc. & Communication System shall not be considered for calculating system availability. However, RTU, communication equipment's auxiliary power supply shall be tested as per the provisions given in their respective chapters.

The SCADA system (hardware and software systems) shall be available for 99% of the time during the 360hours (15 days) test period. However, there shall not be any outage /down time during last 85 Hours of the test duration. In case the system availability falls short of 99%, the contractor shall be allowed to repeat the system availability test after fixing the problem, failing which the system shall be upgraded by the contractor to meet the availability criteria without any additional cost implication to the owner.

Availability tests of RTUs shall be conducted along with System availability test for 360 hours. Each RTUs shall exhibit minimum availability of 99%. In case the RTU availability falls short of 99%, the contractor shall be allowed to repeat the RTU availability test (for failed RTU only) after

fixing the problem, failing which the equipment shall be upgraded by the contractor to meet the availability criteria without any additional cost implication to the owner.

In the event of unsuccessful reruns of the availability test, NEA may invoke the default provisions described in the General Conditions of Contract.

The system availability tests will be performed by the owner by using the SCADA system and RTUs for operation, control and monitoring of the system and using Contractor supplied documentation. The owner will also be required to generate daily, weekly and monthly reports. The supplied system shall be operated round the clock.

The SCADA system shall be considered as available if

(a) One of the redundant hardware is available so that all the applications are functional to ensure the design & performance requirement as envisaged in the specification

(b) At least one of the operator console is available

(c) At least one of the printers is available (off-lining of printers for change of ribbon, cartridge, loading of paper, paper jam shall not be considered as downtime)

(d) All SCADA applications are available

(e) All SCADA functions described in the specification are executed at periodicities Specified in the specification. without degradation in the response times

(f) Requests from available Operator Consoles & VPS are processed

(g) Information Storage and Retrieval applications are available

(h) Data exchange with other system is available

(i) DC/DR data exchange and synch at defined periodicity , However, each device, including servers, shall individually exhibit a minimum availability of 99%.

The non-availability of following non-critical functions shall not be considered for calculations of system availability; however, these functions should be available for 99% of the time.

(a) Database modification and generation

(b) Display modification and generation

(c) Report modification and creation

(d) DTS

During the availability test period, NEA 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.

The successful completion of system availability test at site shall be considered as **"Operational acceptance"** of the system.

7.5.1 Downtime

Downtime occurs whenever the criteria for successful operation are not satisfied. During the test period, owner shall inform the Contractor for any failure observed. For attending the problem the contractor shall be given a reasonable travel time of 8 hours. This service response time shall be treated as hold time and the test duration shall be extended by such hold time. The downtime shall be measured from the instant, the contractor starts the investigation into the system and shall continue till the problem is fixed. 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. Contractor shall be allowed to use mandatory spares (on replenishment basis) during commissioning & availability test period. However, it is the contractor's responsibility to maintain any additional spares as may be required to maintain the required system availability individual device/ equipment availability. All outage time will first be counted but if it is proven to be caused by hardware or software not of Contractor's scope, it will then be deducted.

7.5.2 Holdtime

During the availability test, certain contingencies may occur that are beyond the control of either NEA or the Contractor. These contingencies may prevent successful operation of the system but are not necessarily valid for the purpose of measuring SCADA availability. Such periods of unsuccessful operation may be declared "holdtime" by mutual agreement of NEA and the Contractor. Specific instances of holdtime contingencies could be Scheduled shutdown of an equipment, Power failure to the equipment, Communication link failure.

7.6 Documentation

The complete documentation of the systems shall be provided by the contractor. Each revision of a document shall highlight all changes made since the previous revision. NEA's intent is to ensure that the Contractor supplied documentation thoroughly and accurately describes the system hardware and software.

The contractor shall submit the paper copy of all necessary standard and customized documents for SCADA in 2 sets for review/approval by the NEA for necessary reference which includes the following:

(a) System overview document

(b) Cross Reference Document

(c) Functional design document

(d) Standard design documents

(e) Design document for customization

(f) System Administration documents- software utilities, diagnostic programs etc.

(g) Software description documents

(h) Bill of Quantity & List of software and hardware deliverable

(i) protocol implementation documents

(j) point address document

(k) IP addressing plan document

(l) Software User document for dispatchers

(m) Software Maintenance document

(n) Training documents

(o) Real time & RDBMS documents

(p) Database settings, Displays and Reports to be implemented in the system

(q) Test procedures

(r) Test reports

(s) Hardware description documents

(t) Hardware User documents

(u) Hardware Maintenance documents

(v) Data Requirement Sheet (DRS) of all Hardware

(w) Site specific Layout, Installation, GA, BOQ, schematics and cabling details drawings/documents

(x) Cyber Security Plan

(y) Interoperability profiles/ Tables

After approval two sets of all the above documents as final documents shall be delivered to site by the Contractor. In case some modifications/corrections are carried out at site, the contractor shall again submit as built site specific drawings in three sets after incorporating all such corrections as noticed during commissioning. Any software modifications/updates made at site shall also be documented and submitted in three sets to site and one set to NEA.

In addition to paper copies, two sets of final documentation shall be supplied on electronic media to NEA. The contractor shall also submit two sets of the standard documentation of Operating system and Databases in electronic media. Paper copies of these may be submitted, if the same are available from the OEM as a standard part of delivery. One copy of the software packages used for accessing & editing the final documentation in electronic media shall also be provided.

------End of Chapter 7-----

CHAPTER 8: TECHNICAL REQUIREMENTS OF RTU

8.0 General

The Remote Terminal Unit (RTU) shall be installed at primary substation to acquire data from Multifunction Transducers (MFTs), discrete transducers & status input devices such as CMRs etc. RTU shall also be used for control of Substation devices from Master station(s). The supplied RTUs shall be interfaced with the substation equipment's, communication equipment's, power supply distribution boards; for which all the interface cables, TBs, wires, lugs, glands etc. shall be supplied, installed & terminated by the Contractor.

8.1 Design Standards

The RTUs shall be designed in accordance with applicable International Electro- technical Commission (IEC), Institute of Electrical and Electronics Engineer (IEEE), American National Standards Institute (ANSI), and National Equipment Manufacturers association (NEMA) standards, unless otherwise specified in this technical specification. In all cases the provisions of the latest edition or revision of the applicable standards in effect shall apply.

The RTU shall be designed around microprocessor technology. For easy maintenance the architecture shall support pluggable modules on backplane. The field wiring shall be terminated such that these are easily detachable from the I/O module. The RTU shall comply to IEC62351- 3/ IEC62443-4-2 standard for cyber security.

8.2 RTU Functions

All functional capability described herein shall be provided by the Contractor even if a function is not initially implemented.

As a minimum, the RTU shall be capable of performing the following functions:

(a) Acquiring analog values from Multifunction Transducers or alternatively through transducer- less modules and the status inputs of devices from the substation, processing and transmitting to Master stations. Capability to acquire analog inputs from analog input cards receiving standard signals viz current loops **4-20mA DC & volage signals such as 0-5 V DC. 0-10 V DC etc. For RTD, transducers (for pressure, temperature transducers) etc.**

(b) Receiving and processing digital commands from the master station(s)

(c) Data transmission rates - 300 to 19200 bps for Serial ports for MODBUS. and 10/100 **Mbps** for TCP/IP Ethernet ports

(d) IEC 60870-5-104 protocol to communicate with the Master station(s) at least **2 port,** IEC 60870-5-101 for slave devices & MODBUS protocol over RS485 interface to communicate with the MFTs. If considered as a part of RTDAS/SCADA solution to use IEC-20922 for real time monitoring/control using IEC-20922 can be additionally and optionally, used with GPRS also subject to meeting performance , functional & security requirement, Nevertheless, system shall have communication capability of 104 also at Control Centre.

(e) RTU shall have the capability of automatic start-up and initialization following restoration of power after an outage without need of manual intervention. All restarts **status** shall be reported to the connected master stations.

(f) Remote database downloading of RTU from master station/SCADA control center

(g) Act as data concentrator on IEC60870-5-101/103/104/MODBUS(h) Internal battery backup to hold data in SOE buffer memory & also maintaining the time & date.

(h) As the SCADA system will use public domain such GPRS/MPLS-4G/CDMA etc., therefore it mandatory to guard the data/ equipment from intrusion/damage/breach of security & shall have SSL/VPN based security.

(i) Shall have SNMP

(j) Conformance to IEC62351-3/ IEC62443 standard for cyber security

(k) All RTU's should support IEC-61850 protocols.

Support Feature:

All support feature as mentioned below will not be used now & may require in future. However, the same shall be tested in routine /Factory Tests. Further, it should be possible to have following capabilities in the RTU by way of addition of required hardware limited to addition of I/O modules & communication card or protocol converter & using the same firmware at later date:

(a) Support for Analog output in form of standard current loops viz 4-20mA etc Support for IEC61850 /protocols & ability to act as a gateway for Numerical relays/ Smart Meters may have to be interfaced if need be

(b) Have required number of communication ports for simultaneous communication with Master station(s), /MFTs and RTU configuration & maintenance tool.

(c) PLC support

(d) Communication with at least two master stations simultaneously on IEC 60870-5-104

(e) Receiving and processing analog commands from master station(s) and Capability of driving analog output card.

(f) RTU shall be capable of acquiring analog values through transducers having

(g) Output as 4-20 mA, 0-10 mA, 0-+10 mA or +/- 5 volts etc. using analog input modules.

(h) Capability of time synchronization with GPS receiver which may be required future.

8.3 Communication ports

The RTUs shall have the following communication ports to communicate with master station, existing /MFTs and configuration & maintenance terminal.

a. RTU shall have two TCP/IP Ethernet ports for communication with Master station(s) using IEC 60870-5-104.

b. RTU shall have required number of RS 485 ports for communication with MFTs to be connected in daisy chain using MODBUS protocol. Minimum 15 analog values (including 4 energy values) to be considered per energy meter The RTU shall be designed to connect maximum 5 MFTs. Further, the bidder to demonstrate during testing that all analog values

updated within 2 sec. The updation time shall be demonstrated during FAT(routine) & SAT testing . The bidder can offer MFT on IEC 60870-101/104 protocol to communicate with RTU.

c. In addition, if weather transducer & DC transducers are also having RS485

d. RTU shall have one port for connecting the portable configuration and maintenance tool for RTU.

e. RTU should act as a data concentrator, then RTU shall have additional communication ports Ethernet or serial for IEC60870-5-104/101 using SSL/VPN

f. Secure Gateway Capability: The RTU communication modules shall support built-in hardware-based encryption (IPSec/SSL VPN) to ensure secure data transmission over public networks (GPRS/4G). The module shall be capable of operating as a Secure IoT Gateway, supporting routing and firewall features directly at the substation level to prevent unauthorized access.

It shall be possible to increase the number of communication ports in the RTU by addition of cards, if required in future. The RTU shall support the use of a different communication data exchange rate (bits per second) and scanning cycle on each port & different database for each master station

8.3.1 Master Station Communication Protocol

RTU shall use IEC 60870-5-104 communication protocol for communicating to master station. The RTU communication protocol shall be configured to report analog (except energy values) & status changes by exception to master stations. However, RTU shall support periodic reporting of analog data and periodicity shall be configurable from 2 sec to 1 hour. Digital status data shall have higher priority than the Analog data. The dead-band for reporting Analog value by exception shall be initially set to 1% (user configurable) of the full scale value. In addition, analog values shall also be reported to Master station by exception on violation of a defined threshold limit. All the analog values and status data shall also be assigned to scan groups for integrity check by Master stations at every 10 minutes configurable up to 60 minutes RTU wise.

RTU shall report energy values to master station periodically. The periodicity shall be configurable from 5 minutes to 24 hours (initially set for 15 minutes)

8.3.2 Communication Protocol between RTU & MFTs

The RTU shall acquire data from the MFTs using the MODBUS protocol. In addition, usage of IEC 60870-5-101/104 protocols is also permitted. The MFT will act as slave to the RTU. The RTU shall transmit these values to the master station in the frame of IEC 60870-5-104/101 protocol. As an alternate approach the NEA/contractor may use RTU as a data concentrator & acquire all the required analog data from DCU installed & connected to energy meters using MODBUS /DLMS as legacy system . However, performance, functional, availability & update time requirement shall be met in this case also. It is the responsibility of NEA /contractor to assess this option & only opt in case it is found feasible,

8.4 Analog Inputs

The real time values like, Active power, Reactive Power, Apparent power three phase Current & Voltage and frequency, power factor & accumulated values of import /export energy values will be acquired RTU from the following in the given manner:

1. MFTs installed in substations
2. RTU shall also take 4-20 mA, 0-20mA, 0- -10mA, 0-+10mA, 0-5V etc.as analog inputs to acquire transformer tap position, DC power supply voltage, weather transducer etc.

The RTU analog-to-digital (A/D) converters shall have a digital resolution of at least twelve (12) bits plus sign. The overall accuracy of the analog input system shall be at least 0.2%(i.e. 99.8%) at 25 ºC of full scale . Mean accuracy shall not drift more than 0.002% per degree C within the temperature range of –5-to-+55-degree Linearity shall be better than 0.05%. The RTU shall be designed to reject common mode voltages up to 150 Vac (50 Hz). For dc inputs, normal mode noise voltages up to 5 Vac shall be rejected while maintaining the specified accuracy. Each input shall have suitable protection and filtering to provide protection against voltage spikes and residual current at 50 Hz, 0.1 ma (peak-to-peak) and overload. Loading upto 150% of the input value shall not sustain any failures to the RTU input.

The ability of the RTU to accommodate dc inputs shall include the following signal ranges:

Unipolar Voltage:0-0.5V, 0-1V, 0-5V, 0-10V, Unipolar Current:0-1mA, 0-10mA,0- 20mA, 4-20Ma, Bipolar Voltage: 0.5V, 2.5V, 5V, -20-0-20mA (- to +)

The total burden imposed by the RTU/DC analog input circuit shall not exceed 0.5 volt-ampere for current and voltage inputs. As an option, the contractor may also provide transducer less solution to connect direct CT/PT secondaries.

8.5 Status input

RTU shall be capable of accepting isolated dry (potential free) contact status inputs. The RTU shall provide necessary sensing voltage, current, optical isolation and de-bounce filtering independently for each status input. The sensing voltage shall not exceed 48Vdc.

The RTU shall be set to capture contact operations of 20 ms or more duration. Operations of less than 20 ms duration shall be considered no change (contact bounce condition). The RTU shall accept two types of status inputs i.e. Single point Status inputs and Double point status inputs.

To take care of status contact chattering, a time period for each point and the allowable number of operations per time period shall be defined. If the allowable number of operations exceed within this time period, the status change shall not be accepted as valid

Single point status input will be from a normally open (NO) or normally closed

(NC) contact which is represented by 1-bit in the protocol message.

The Double point status input will be from two complementary contacts (one NO and one NC) which is represented by 2-bits in the protocol message. A switching device status is valid only when one contact is closed and the other contact is open. Invalid states shall be reported when both contacts are open or both contacts are closed.

All status inputs shall be scanned by the RTU from the field at 1 millisecond periodicity.

8.6 Sequence of Events (SOE) feature

To analyze the chronology or sequence of events occurring in the power system, time tagging of data is required which shall be achieved through SOE feature of RTU. The RTU shall have an internal clock with the stability of 10ppm or better. The RTU time shall be set from time synchronization messages received from master station using IEC 60870-5- 104 protocol. In addition, the message can be transmitted using NTP/SNTP. SOE time resolution shall be 1ms or better

The RTU shall maintain a clock and shall timestamp the digital status data. Any digital status input data point in the RTU shall be assignable as an SOE point. Each time a SOE status indication point changes the state, the RTU shall time-tag the change and store in SOE buffer within the RTU. A minimum of 1000 events can be stored in the SOE buffer. SOE shall be transferred to Master Station as per IEC 60870-5-104 protocol. SOE buffer & time shall be maintained by RTU on power supply interruption.

8.7 IED pass through

The Master Station user shall be able to perform a virtual connection with any IED connected to the RTU/DC, provided the communication protocol functionality, to support the information transfer from and to the IEDs. For example, the Master Station shall gather on-demand IED data, visualize IED configuration parameters, and IED source code depending upon the IED capabilities. On the other hand, the Master Station shall be able to download to the IEDs configuration parameters, code changes, etc. depending upon the IED capabilities. This feature is a support function considering in future implementation. The capability can be demonstrated with the upload & download of data from master station with IEDs connected to the RTUs using the support of protocols specified in this chapter. Numerical relays Analog data viz voltage ,current, sag swell instantaneous, momentary , temporary, over voltage, under voltage, over current , phasor measurement , THD, current TDD & current unbalance ratio etc. at numerical relays if installed at bay of S/S

8.8 PLC capability

The RTU shall be provided with programmable logic capabilities supported by easy to use editor facilities. The programmable logic capability shall enable the RTU to perform control functions using ladder logic language conforming IEC 1131.

8.9 Control Outputs

The RTU shall provide the capability for a master station to select and change the state of digital output points. These control outputs shall be used to control power system devices such as Circuit breakers relay disable/enable and other two-state devices, which shall be supported by the RTU.

A set of control outputs shall be provided for each controllable device. On receipt of command from a master station using the select check-before-execute operate (SCBO) sequence, the appropriate control output shall be operated for a preset time period which is adjustable for each point from 0.1 to 2 seconds.

Each control output shall consist of one set of potential free NO contact. The output contacts shall be rated at least 0.2 Amp. at 48 Vdc. These output contact shall be used to drive heavy duty relays. In case Control output module of RTU does not provide potential free control output contact of this rating, then separate control output relays shall be provided by the contractor. These relay coils shall be shunted with diodes to suppress inductive transients associated with energizing and de-energizing of the relay coils & shall conform to the relevant IEC requirements.

8.9.1 Heavy duty control output relays

The control output contact from the RTU shall be used for initiating heavy duty relays for trip/close of switching devices and energizing relays of OLTC raise lower. The contractor shall provide heavy duty relays. Each control output relays shall consist of at least 2 NO contacts. The output contacts shall be rated for at least 5 Amps Continuous at 220Vdc and shall provide arc suppression to permit interruptions of an inductive load. Relay coils shall be shunted with diodes to suppress inductive transients associated with energizing and de-energizing of the relay coils. The relays shall conform to the IEC255-1-00 and IEC 255-5 requirements.

8.9.2 Control Security and Safety Requirements

The RTU shall include the following security and safety features as a minimum for control outputs:

(a) Select- check-before-operate operate (SCBO) sequence for control output.

(b) No more than one control point shall be selected/executed at any given time.

(c) The control selection shall be automatically cancelled if after receiving the “control selection" message, the "control execute" command is not received within the set time period.

(d) No control command shall be generated during power up or power down of RTU.

8.9.3 Local/Remote selector switch

A manual Local/Remote selector switch shall be provided for each RTU to disable all control outputs by breaking the power supply connection to the control outputs. When in the "Local" position, the Local/Remote switch shall allow testing of all the control outputs of RTU without activating the control outputs to field devices. A status input indication shall be provided for the Local/Remote switch to allow the SCADA system to monitor the position of the switch.

8.9.4 Dummy breaker latching relay

The Contractor shall provide a latching relay to be used to simulate and test supervisory control from the Master station. The latching relay shall accept the control signals from the RTU to open and close and shall provide the correct indication response through a single point status input.

8.10 Contact Multiplying Relays (CMRs)

Contact Multiplying Relays (CMRs) are required to multiply the contacts of breaker and protection relays etc. The contacts of these relays shall be used to provide status inputs to the RTUs.

The relays shall be DC operated, self-reset type. The rated voltage for relay operation shall be on 24/48/110/220V DC depending on the station DC supply. The relay shall be able to operate for +/- 20% variation from nominal voltage.

The relay shall have a minimum of two change over contacts, out of which one shall be used for telemetry purposes. The contacts shall be rated to carry minimum current capacity of 5A. The relay shall conform to following requirement.

a) Power Frequency withstand voltage–2KV for 1 minute as per IEC 255-5.

b) Insulation Resistance of for ohms measured using 500V DC megger.

c) 5KV Impulse test as per IEC 255-5

The relays coils shall be shunted with diodes to suppress inductive transients associated with energizing and de-energizing of the relay coils. The relays shall conform to the IEC 255-1-00, IEC 255-5 requirements. The relays must be protected against the effects of humidity, corrosion & provide with a dust tight cover. The connecting terminals shall be screw type & legibly marked. The relays may optionally have a visual operation indicator. The relays are to be mounted in Control & Relay (C&R) panels and therefore shall be equipped with suitable mounting arrangements. In case suitable space is not available in C&R panel the same shall be mounted in RTU panel or suitable panels , which shall be supplied & mounted on the top of the C&R panel by the contractor.

8.11 Time facility

The internal RTU time base shall have a stability of 10 ppm. The RTU shall be synchronized through synchronization message from master station at every 15 minutes (configurable from 15 minutes to 24hrs) over IEC 60870-5-104/101/NTP/SNTP. The RTU shall also carry out time stamping of the events which are not received as time stamped from connected IEDs etc.

8.12 Diagnostic Software

Diagnostic Software shall be provided to continuously monitor operation of the RTU and report RTU hardware errors to the connected master stations. The soft- ware shall check for memory, processor, and input/output ports errors and failures of other functional areas defined in the specification of the RTU.

8.13 SCADA language based on IEC61131-3

RTU shall have capability to write various programs based IEC 61131-3 SCADA language. It will facilitate users to write various programs using points defined in the database

.

8.14 Input DC Power Supply

The RTU will be powered from a 48 V DC power supply system. The RTU shall not place additional ground on the input power source. The characteristics of the input DC power supply shall be

(a) Nominal voltage of 48 Vdc with variation between 40.8 and 57.6 V DC.

i.e. 48(+20%/-15%)

(b) (Maximum AC component of frequency equal to or greater than 100 Hz and

0.012 times the rated voltage peak-to-peak.

The RTU shall have adequate protection against reversed polarity, over current and under voltage conditions, to prevent the RTU internal logic from being damaged and becoming unstable causing mal operation. The RTU's shall operate at 48V DC / 110V DC. The permissible ranges as per applicable standards specified shall be adhered to accordingly. The interface components like CMRs, HDRs MFT etc. may also be selected accordingly.

At each old and new substations 110v DC will be available for RTU's, the bidder may propose their RTU design based on the available voltage levels at each substations. The bidder may either choose 48V RTU with 110V DC to 48 V DC converted or RTU's compatible for 110v DC, for their proposed solution.

8.15 Environmental Requirements

The RTU will be installed in control room buildings with no temperature or humidity control. The RTUs shall be capable of operating in ambient temperature from-20 to +60 degree C with rate of temperature change of 20 degree C/hour and relative humidity less than 95%, non- condensing. For RTUs to be installed in the hilly region with the history of snowfall, the lower ambient temperature limit shall be -10 degree C. NEA may specify location with altitude more than 2000m above MSL for compliance of RTUs to be installed in that project area

8.16 RTU Size and Expandability

RTU shall be equipped for the point counts defined in the BOQ (Basic+20% spare (wired & hardware). It shall be possible to expand the RTU capability for additional 100 % of the basic point counts by way of addition of hardware such as modules, racks, panels, , however, RTU software and database shall be sized to accommodate such growth without requiring software or database regeneration.

8.17 RTU Panels

At least 50% of the space inside each enclosure shall be unused (spare) space that shall be reserved for future use. The Contractor shall provide required panels conforming to IEC 529 for housing the RTU modules/racks, relays etc. and other required hardware. The panels shall meet the following requirements:

(a) RTU shall be free-standing, floor mounted and height shall not exceed 2200 mm. All doors and removable panels shall be fitted with long life rubber beading. All non- load bearing panels/doors shall be fabricated from minimum 1.6 mm thickness steel sheet and all load bearing panels, frames, top & bottom panels shall be fabricated from minimum 2.0 mm thickness steel sheet

(b) RTU shall have maintenance access to the hardware and wiring through lockable full height doors.

(c) RTU shall have adequate cooling fan accordance with the capacity on every RTU Panel.

(d) RTU shall have the provisions for bottom cable entry

(e) The safety ground shall be isolated from the signal ground and shall be connected to the ground network. Safety ground shall be a copper bus bar. The contractor shall connect the panel's safety ground of to the owner's grounding network. Signal ground shall be connected to the communication equipment signal ground.

(f) All panels shall be supplied with 230 Vac, 50 Hz, single-phase switch and 15/5A duplex socket arrangement for maintenance.

(g) All panels shall be provided with an internal maintenance lamp, space heaters and gaskets.

(h) All panels shall be indoor, dust-proof with rodent protection, and meet IP41 class of protection.

(i) There shall be no sharp corners or edges. All edges shall be rounded to prevent injury.

(j) Document Holder shall be provided inside the cabinet to keep test report, drawing, maintenance register etc.

(k) 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.

8.18 Wiring/Cabling requirements

The RTU panels shall gather all signals from and to the devices located in Control & Relay panels in the substation control room. All wires that carry low-level signals shall be adequately protected and separated as far as possible from power wiring. All wires shall be identified either by using ferrules or by color coding. In addition, cables shall be provided with cable numbers at both ends, attached to the cable itself at the floor plate where it enters the cubicles.

Shielded cables shall be used for external Cabling from the RTU panels. The external cables (except communication cables) shall have the following characteristics:

(a) All cables shall have stranded copper conductor.

(b) Minimum core cross-section of 2.5 mm for PT cables, 4 mm2 for CT cables, if applicable and 2.5 mm2 for Control outputs and 1.5mm2 for Status inputs

(c) Rated voltage Uo/U of 0.6/1.1KV

(d) External sheathing of cable shall have oxygen index not less than 29 & temperature index not less than 250. Cable sheath shall meet fire resistance test as per IS 1554 Part- I.

(e) Shielding, longitudinally laid with overlap.

(f) Dielectrics withstand 2.5 kV at 50 Hz for 5 minutes

(g) External marking with manufacture's name, type, core quantity, cross-section, and year of manufacture.

(h) Armored Cables shall be used in the area where cable will pass through open area which may experience loading.

(i) The Communication cable shall be of shielded twisted pairs and of minimum0.22sqmm size.

8.19 Terminal Blocks (TBs)

Terminal blocks shall be having provision for disconnection (isolation), with full depth insulating barriers made from moulded self-extinguishing material. Terminal blocks shall be appropriately sized and rated for the electrical capacity of the circuit and wire used. No more than two wires shall be connected to any terminal. Required number of TBs shall be provided for common shield termination for each cable.

All terminal blocks shall be suitably arranged for easy identification of its usages such as CT circuits, PT circuits, analog inputs, status inputs, control outputs, auxiliary power supply circuits, communication signals etc. TBs for CT circuits shall have feature for CT shorting (on CT side) & disconnection (from load side) to facilitate testing by current injection. Similarly, TBs for PT circuit shall have feature for disconnection to facilitate voltage injection for testing.

8.20 RTU Architecture

Bidder has the option to offer RTUs having following architectural design:
(a) Centralized RTU design where all I/O modules are housed in RTU panels and communicating

with master station through communication port.

(b) Distributed RTU design where distributed I/O modules /processor with I/O modules are housed in respective bay panels/RTU panel. All these distributed I/O modules / I/O modules with processor shall be connected to a central processor for further communication with master station. The bidder shall assess the requirement of RTU panels for such design and supply panels accordingly. This is applicable for Numerical replay/BCPU concept.

In both cases the RTU requirements as envisaged in this specification shall be followed.

8.21 Local Data Monitoring System (LDMS)

The LDMS shall be installed at each substation to provide real-time monitoring, data acquisition, control, event logging, and communication diagnostics for field equipment interfaced with the RTU system. It shall operate as a standalone system, capable of functioning independently in case of communication loss with the Central SCADA.

The system shall log all alarms, events, and user actions with time synchronization from GPS or master clock, and provide facilities to filter, acknowledge, and export alarm/event data in CSV or PDF format. The LDMS shall support real-time and historical trending of analog parameters (e.g., voltage, current, power, temperature) and generate auto-configurable daily and shift reports for operator review.

The LDMS shall interface with local RTU/PLC using standard protocols such as IEC 60870-5-101/104, Modbus TCP/IP, DNP3.0, or IEC 61850, as per project requirements. The software shall be installed on an industrial-grade workstation or server at each substation, with a secure and open operating system (e.g., Windows Server or Linux).

8.22 RTU Earthing

(a) Bidder shall provide a separate maintenance free low resistance (<1 ohm) Clean earth substation for RTUs and SCADA Equipment ensuring reliable operation, surge protection and personal sa

(b) The RTU body/frame shall be suitably connected to the separate earth.

(c)

(c) The bidder shall have overall responsibility to ensure that the RTU earthing arrangement is suitably designed to prevent failures of electronic cards and other components in the RTU.

(d) **Reference Standards**

IS 3043, IEEE Std 142, IEC 60364, and manufacturer recommendations.

8.23 110VDC to 48VDC Converter for RTU

The RTU Power Supply module shall preferably accept **110 V DC (Station Battery Voltage) directly** to ensure high reliability. If the proposed RTU architecture only supports 48 V DC, the Contractor must supply a redundant, industrial-grade DC-DC converter (110V to 48V) with adequate surge protection and isolation.

-----End of Chapter 8-----

CHAPTER 9: TRANSDUCER & MODEM REQUIREMNTS

9.0 Transducer Requirements:

All transducers shall use a 110 Vdc / 48 Vdc auxiliary power supply as provided for the RTU and applicable values /limits/ permissible test values shall be considered as per nominal value of voltage. Optionally, MFTs can also be self-powered. Transducer shall be din rail or wall/plate mounted.

The input, output and auxiliary circuits shall be isolated from each other and earth ground. The transducer output shall be ungrounded and shall have short circuit and open circuit protection. The transducers shall comply to the following requirements, in addition to the requirement of IEC 60688, without damage to the transducer.

(a) Voltage: Voltage test and other safety requirement compliance as specified in IEC 60688 or 60687and IEC 414.

(b) Impulse Withstand:

IEC 60688 or 60687compliance is required.

(c) Electromagnetic Compatibility:

IEC 60688 or 60687 and IEC 801-3, level 1 compliance required.

(d) Permanent Overload Protection:

IEC 60688 or 60687 compliance is required.

(e) Temporary Overload Protection:

IEC 60688 or 60687 compliance is required.

(f) High Frequency Disturbance:

IEC 60688 or 60687 compliance is required.

The transducers shall comply with the following general characteristics:

(a) Shock Resistance:

Minimum severity 50 A, IEC 68-2-27 requirements

(b) Vibration Strength:

Minimum severity 55/05, IEC 68-2-6 requirements.

(c) Input Circuit Consumption:

Less than or equal to 0.2 VA for voltage and 0.6VA for current circuits.

(d) Reference Conditions for Accuracy Class: IEC

60688 or 60687compliance is required.

(e) Temperature Rise:

IEC 60688 or 60687 compliance is required.

(f) Operating Temperature:

0 degree C to + 60 degree C (-5 o C to + 55 o C for project area with snowfall

history)

9.1 Multi-Function Transducers (MFTs)

The contractor shall provide the multi-function transducers for acquiring the real time analog inputs through 3 phase 3 wire CT/PTs circuits/ 3 phase 4 wire CT/PTs circuits (Based on the field requirement). Based on the CT/PT secondary rating, the multi-function transducer shall be designed for nominal 110 V (Ph to Phase) and 1A/5A (per phase current). The MFT shall be suitable for 20% continuous overload and shall be able to withstanding 20 times the normal current rating for a period one second. The MFT shall be able to accept the input voltages upto 120% of the nominal voltage. The MFT shall have low VA burden. MFTs shall be mounted in the interface cabinet to be supplied by the contractor.

Multi-function transducers shall provide at least phase voltage, phase current active/reactive power, import & export energy (active & reactive), pf , frequency with class 0.5 accuracy or better.

The parameters to be acquired from multifunction transducers shall be selectable. MFT shall provide the 15 minute values (configurable 15 minute/1 hour) of Active Energy Import, Active Energy Export, Reactive Energy Import and Reactive Energy Export.

Multi-function transducers shall accept nominal 48 V / 110 V DC as auxiliary power supply. Optionally, MFT can be self-powered also. Multi-function transducer shall be provided with RS485 interface to communicate with RTU over Modbus protocol in multi-drop mode. Optionally, the MFT with IEC60870-5-101/104 can be used.

The MFTs shall be suitable for mounting on DIN rails. The MFT terminals shall accept upto two 2.5 mm2 / 4 mm2 for PT/CT circuit terminations as applicable.

The MFT shall be programmable with password protection thru suitable facia mounted keypad arrangement so that the configuration parameters such as CT/PT ratio , integration time of energy , reset, communication parameters setting (Address, baud , parity) can be set up at site also. The device shall have LCD displays to visualize all parameters being monitored & configuration etc. have configurable at site for CT/PT ratio etc.

9.2 DC Transducer

The DC transducer (DCT) are following types.

(a) Voltage

(b) Current

(c) Winding Temp

(d) Oil temp

The DC Transducer are required to measure battery charger current & voltage shall be suitable for 20% continuous overload and shall be able to withstanding 20 times the normal current rating for a period one second. The DCT shall be able to accept the input upto 120% of the nominal voltage. The DCT shall have low VA burden. DCT shall be mounted in the interface cabinet to be supplied by the contractor. The input range for current & voltage are site specific & hence the same shall be specified RFP floated by NEA/state Output of the device shall preferably be 4-20ma or MODBUS in order to optimize the BOQ. However, as specific cases the output in line ranges specified in analog input card.The accuracy of transducer shall be ±0.5%

9.3 Transformer Tap Position Transducer (OLTC)

The transformer tap position indications shall be either of two types based on field requirement.

i. Variable resistance type

ii. Lamp type

The Contractor shall provide suitable resistance tap position transducers which shall have the following characteristics

(a) The input measuring ranges shall be from 2 to 1000 ohms per step, which is tunable at site with at least 25 steps.

(b) Dual output signal of 4 to 20 mA DC, 0.5% accuracy class as per IEC 688 shall be provided. One output will be used for driving a local digital indicator (to be provided by the contractor) and the other will be used for interfacing with the RTU. Alternatively, for RTU, MODBUS link may be used. In case of lamp type, additional resistance/potentiometer unit shall be provided to convert the dry type contacts to a variable resistance as defined in (a) above, suitable for the remote indication

9.4 Modems

(a) The modem shall have suitable interface facility to connect with the RTU. It shall have dual SIM facility.

(b) The offered Modem should be capable of transferring the entire data as per the data requirement of RTU at control center i.e. 4G /5G as per site signal condition

(c) The offered Modem should be supplied with power cable, antenna with co-axial cable of length, RS 232 /485connecting suitable cable, mounting adopter etc

(d) Sealing :- The modem cover and body should have arrangement for sealing. In addition to this, the SIM card holder cover should also have arrangement for sealing.

(e) Antenna :- The Modem should have flexible external antenna to enable placement of the antenna at the location of strongest signal inside the Metering Cubicle. Bidders are requested to quote separately for multiple gain antenna, such as 0dBi/3dBi/10dBi with screw mount / Wall mount arrangement. The actual requirement of these Modem Antennas of various gains may vary as per the requirement at site. Bidder will be required to supply the exact requirement as per site conditions and will be paid as per the separate unit rated quoted for different Gain Antennas.

(f) Before supply of GSM/CDMA modem, the bidder is requested to ensure the availability of appropriate signal and operation of GSM/CDMA Modem in all the areas to be covered by making physical survey or otherwise. Before making the actual supply of Modems for RTU locations , the Bidder is requested to assess the exact. requirement and should supply a high gain antenna or any other suitable alternate communication network for collecting data in such area.

(g) In the event of an outage, the modem should be able to initiate separate call or send SMS to predefined number to notify the outage event with data and time of occurrence and restoration

(h) The Modem should act a completely transparent channel i.e. the Commands received from SCADA Control center should be conveyed to RTU and data from RTU should be conveyed to SCADA control center without any changes in the modem.

(i) Data should not reside in the modem before the time of transmission to Control center, to avoid chances of tampering of data at Modem end.

(j) The Modem should be capable of operating with SIMs of local GSM/CDMA Service

(k) provider in the area.

(l) Modem should be capable for continuous working for 24 hours every day under field conditions

(m) (Modem should be a compact model housed in a polycarbonate /engineering plastic

(n) Modem should be Dual Band modem capable of operating at 900 and 1800 MHz

(o) transmission. GSM Modem should support both Data and SMS transmission. It should have both GSM and GPRS/MPLS-4G/EDGE feature

(p) Modem should have an RS232 Interface through a 9 pin or 15 pin D type Connector for connection to RTU. The SIM interface should be a 3 V Interface in accordance with GSM 11.12 phase 2 with a retractable SIM cardholder, which should be fully inserted inside the modem. The holder opening should have a sliding cover with provision for sealing after placing of the SIM card. The modem shall accept the standard SIM Card. Modem should have a SMA Antenna connector

(q) Storage Temperature: -20 degrees to +70 degree Celsius

(r) Operating Temperature: -10 degrees to +60 degree Celsius

(s) Humidity:- - 95% RH (Non - Condensing)

(t) NEA may specify location with altitude more than 2000m above MSL for compliance of RTUs to be installed in that project area

(u) Maximum Power Output should be 2 W at 900 MHz (Class 4) and 1W at 1800 MHz

(v) (Class 1).

(w) Sensitivity :- GSM 900 : <-100 dBm GSM 1800 : <-100 dBm

(x) Standard AT Command set (GSM 07.05, GSM07.07)

(y) TCP/IP stack access via AT

(z) Internet Services : TCP, UDP, HTTP, FTP, SMTP, POP3

(aa) Max. Baud Rate: for GSM -9600

(bb) GPRS/MPLS-4G Class B Multi slot class 12 or class B Multi slot class 10 Packet channel

(cc) support : PBCCH

(dd) EDGE (EGPRS/MPLS-4G) Multi slot class12 or Multi slot class 10Mobile station Class B Modulating and coding schemes : MCS 1 to 9 Packet channel support : PBCCH

(ee) SMS Features: - Text and PDU Point to point (MT/MO, Cell broadcast

(ff) The Modem should have LED indications for transmit data, received data carrier detects and Power ON, etc. to indicate Power on position and to indicate the availability of signal at the place of installation.

(gg) The modem should be RTUs buffer data for at least 24 hours in case of communication failure.

(hh) Modem should support following ports:

a) Ethernet Ports – Minimum 1 x RJ45 (10/100 Mpbs) port for RTU connection.

Preferably 2 ports (one spare/service)

b) Serial Ports -1 x RS232/RS485 port for legacy RTU connectivity

c) Antenna Ports – 1 x Main cellular antenna. Optional external antenna

d) Local configuration port – USB/RS232 for local setup via PC

9.5 Substation WAN Router (Field Gateway)

The Router shall be a ruggedized **Industrial Field Gateway** designed for installation inside substation control panels to secure RTU communications.

- Architecture & Environmental:
  - **Form Factor:** Compact, Fanless design suitable for **DIN-Rail mounting**.
  - **Operating Temperature:** Extended industrial range **-40°C to +75°C**.
  - **Power Input:** Dual Redundant DC Power Inputs supporting **110 VDC / 48 VDC** (Station Battery Voltage) directly.
  - **Standards:** IEC 61850-3 and IEEE 1613 compliant for substation environments.
- Performance & Connectivity:
  - **Encrypted Throughput:** Minimum **50 Mbps** (IPSec/SSL VPN).
  - **Interfaces:** Minimum 2 x 10/100/1000 Base-T (RJ45) ports + 1 x Serial Port (RS-232/485) for legacy RTU interfacing.
  - **Cellular Uplink:** Built-in **4G LTE / 5G Modem** with Dual-SIM slots for carrier redundancy.
- Protocols & Security:
  - **Routing:** Support for OSPF, BGP, and VRRP for LAN redundancy.
  - **Security:** Stateful Firewall, IPSec VPN, SSL VPN, and NAT.
  - **SCADA Support:** Built-in serial-to-IP conversion (encapsulation) for legacy DNP3/Modbus devices.
  - **Management:** SNMPv3, HTTPS, and support for Centralized Network Management System (NMS).

outer shall be an **Industrial Services Router** designed for mission-critical SCADA data exchange.

ommunicate with control center through GPRS/MPLS network. The router specification shall be suitable to communicate with Control center. Industrial Grade Router (Managed L2/L3) should support QUAD core 1.2GHz CPU, DRAM of 2GB & usable Flash Memory of 2GB. Should support WAN port on Combo Gigabit Ethernet (RJ45/SFP slot) Gateway should have Four 10/100BASE-T Fast Ethernet LAN ports with 4KV isolation for Electrostatic Discharge (ESD) protection. Router should support 1 RS-232 serial ports Gateway should have mini–Type B USB Console port, Dual SIM for 3G/4G/5G, MAC address filtering.

The Router should have built-in security features like SSL VPN for remote access, Next gen encryption such as AES-256, SHA-384, and SHA-512, IP Sec tunnels, NAT Transparency, VRF Aware Ipsec and Ipsec over IPv6.

Gateway should also have built in firewall features like Zone based policy firewall, VRF-aware stateful inspection routing firewall, Advanced application inspection and control, Dynamic and static port security

Router should have SDWAN so that dynamic path selection feature can be achieved to select the best available path out of multiple routes based on delay, jitter, and latency.

Router should support IPv6 name resolution, IPv6 DHCP and IPv6 NAT features, IP SLA,

OSPFv2 and OSPFv3, BGP & EIGRP.

Router should support IEC 60870 T101, T104 protocol translations. Comply with IEEE 1613 and IEC 61850-3 standards

Router should be able to operate in the temperature range of -40 to 60 degree Celsius. Gateway should support both In-band and out-of-band management using Telnet and SNMP, including MIB II and other extensions. Hazardous certification : ANSI/ISA ,EN

9.5 IEC-61850 to IEC-60870-5-104 Protocol Converter / Gateway

Technical Specification for IEC 61850 to IEC 60870-5-104 Protocol Converter

1. General Requirements

The protocol converter shall be a robust, industrial-grade device designed for continuous operation in a substation or industrial environment. It shall facilitate seamless, two-way communication between devices and systems using the IEC 61850 protocol and a central control system using the IEC 60870-5-104 protocol.

2. Protocol Support

IEC 61850: The converter shall fully support IEC 61850 Edition 2 (backward compatible with Edition 1) for substation automation. It must support both the Client (for GOOSE and MMS) and Server (for MMS) roles. It shall be capable of parsing and using the SCL (Substation Configuration Language) file for configuration.

IEC 60870-5-104: The converter shall function as a Client (master) or Server (slave) to establish a TCP/IP connection with the control center. It must support standard data types and functionalities including:

- Single Point and Double Point indications
- Measured values (with and without time tags)
- Command execution (single and double commands)
- General Interrogation and Counter Interrogation
- Time Synchronization: The converter shall support time synchronization via SNTP or NTP.

3. Hardware Requirements

Design: The device shall be built for industrial use, with a rugged, fanless design for reliable operation in harsh environments.

Mounting: It shall be a DIN rail mountable device.

Power Supply: The device shall operate on a standard industrial DC power supply (e.g., 24VDC or 48VDC) with redundant power input terminals.

Operating Conditions: The converter must be able to withstand a wide temperature range (e.g., -40°C to +70°C) and high humidity without condensation.

Ports: The converter shall have multiple communication ports, including at least:
Two (2) 10/100/1000BaseT Ethernet ports (RJ45) for IEC 61850 and IEC 60870-5-104 communication.

One (1) serial port (RS-232/485) for configuration and management.

-----End of Chapter 9-----

CHAPTER 10 TEST EQUIPMENTS FOR RTU

10.0 RTU Configuration and Maintenance Tool

Test equipment for RTU shall have Configuration and maintenance tool consisting of the followings:

10.1 RTU Data base configuration & Maintenance software tool

The RTU database configuration & Maintenance software tool shall be required to perform the database modification, configuration, compilation and documentation. The database compiler shall provide error detection services. It shall also perform the downloading of the compiled database into the RTU database.

10.2 Master station-cum-RTU simulator & protocol analyzer software tool

The Master station cum RTU simulator tool shall be used to test the communication interfaces of Master station, RTU and Electronic MFT. The Master station simulator tool shall be capable of emulating the master station for IEC 60870-5-104,101 and MODBUS protocols. The RTU simulator shall be capable of emulating the slave protocols for both the IEC 60870-5-104,101, and MODBUS protocols for MFTs. It shall also be possible to prepare illegal messages for transmission, such as messages having invalid checksum.

The protocol analyzer shall be used to monitor all communication traffic on a channel (between Master station & RTU and between RTU & MFT without interfering channels operation. Channel traffic captured in the active or passive modes of operation shall be displayed.

The Master station simulator and protocol analyzer tool shall also have following features:

- Each received message shall be checked for validity, including the check sum. The tool shall maintain and display error counters so that the number of errors during a period of unattended testing can be determined.
- All fields of a message shall be displayed. A pass/fail indication for the message shall be included.

In case of usage of IEC 103/61850/ IEC62056 for data acquisition, the feature of the same also be provided with same or additional tool

10.3 Laptop PC for above software tools along with interfacing hardware

A laptop PC shall be used for the above-mentioned software tools. The laptop PC shall be provided with all hardware accessories including cables, connectors etc. required for interfacing with Master station, RTU and MFT. A suitable Industrial Grade Layer-2 Switch shall be provided to use the tool in monitor mode. A carrying case and a suitable power adaptor (input 230VAC, 50Hz) for laptop PC shall also be supplied.

-----End of Chapter 10-----

CHAPTER 11: TESTING, TRAINING & DOCUMENTATION

11.0 RTU Testing

This chapter describes testing, training & documentation requirement for RTU

(a) Type Testing:

RTU in including Transducers shall conform to the type tests listed in the relevant table. Type test reports of tests conducted in national accredited Labs or internationally accredited labs with in last five years from the date of bid opening may be submitted. In case, the submitted reports are not as per specification, the type tests shall be conducted without any cost implication to NEA. A complete integrated unit shall be tested to assure full compliance with the functional and technical requirements of the Specification including functional requirement. The testing sample shall include one of each type of cards/modules and devices. The list of Type tests to be performed on the RTU is mentioned in **Table-1** & type test requirements are mentioned in **Table-2 of this chapter**. For other items also such as MFT, sensor etc. the requirements are mentioned in the respective sub sections of specification. However, the type tests shall only be limited to the specification of that item only & not as specified for RTU.

(b) Routine Testing or Factory acceptance test (FAT):

Each complete unit shall undergo routine testing. The list of Routine tests to be performed in the factory is mentioned in **Table-2**.

(c) Site Acceptance Test (SAT)

(i) Field Tests

After RTU panel installation, interface cabling with C&R panels/Termination boxes ,communication panel and interface cabling with field & communication equipment, the Contractor shall carry out the field- testing. The list of field tests for RTU is mentioned in **Table-2**

(ii) Availability Tests

After field testing, RTU shall exhibit 99% availability during test period. Availability tests shall be performed along with Master station. The RTU shall be considered available only when all its functionality and hardware is operational. The non-available period due to external factors such as failure of DC power supply, communication link etc., shall be treated as hold-time & availability test duration shall be extended by such hold time.

11.1 Training

The contractor shall provide training to the NEA's personnel. The training program shall be comprehensive and provide for interdisciplinary training on hardware and software. The training program shall be conducted in English. RTU training course shall cover the following:

a) RTU operation including data flow.

b) Troubleshooting, identification and replacement of faulty Modules.

c) Preventive maintenance of the RTU

d) Use of RTU configuration and Maintenance tool

e) All functional and Diagnostic testing of RTU

f) Database modification and configuration of RTU.

11.2 Documentation

The Contractor shall submit 3 sets of all the standard and customized RTU documents for review and approval which includes the following:

a) RTU Function design document

b) RTU Hardware description document & all the documents referred therein to meet all the clauses of the specification.

c) RTU Test equipment user documents

d) RTU user guide

e) RTU Operation & Maintenance document

f) RTU Training Documentation

g) RTU database document

h) RTU I/O list

i) RTU Test procedures

j) Data Requirement Sheet (DRS) of all items

k) Protocol documentation including implementation profile etc.

l) RTU installation and Layout, GA, BOQ, schematics and internal wiring drawings for each RTU site

m) RTU to C&R panels/ field device cabling details for each RTU Site

n) Cyber security compliance certificate /document by manufacturer including international agencies like KEMA / TuV / tested as per NEA.

After approval of all the above documents, the Contractor shall submit three sets as final documents. In case some modifications/corrections are carried out at site, the contractor shall again submit as built site-specific drawings in three sets after incorporating all such corrections as noticed during commissioning of the RTU.

Table-1: List of Tests on RTU

Test Nos.	DESCRIPTION OF THE TEST	Type test	Routine test	Field test
A	**FUNCTIONAL TESTS FOR RTU**			
1.	Check for BOQ, Technical details, Construction & Wiring as per RTU drawings	√	√	√
2.	Check for database & configuration settings	√	√	√
3.	Check the operation of all Analog inputs, Status input & Control output points of RTU	√	√	√
4.	Check operation of all communication ports of RTU	√	√	√
5.	Check for communication with master stations including remote database downloading from master station	√		√
6.	Check for auto restoration of RTU on DC power recovery after its failure	√		√
7.	Test for self-diagnostic feature	√		√
8.	Test for time synchronization from Master	√		√
9.	Test for SOE feature	√		√
10.	End to end test (between RTU & Master station) for all I/O points			√
11.	Test for MODBUS protocol implemented for acquiring data from MFT/ transducers and updation time demonstration in daisy chain configuration	√		√
12.	Test for IEC 60870-5 -104,101 , other protocol implemented	√		√
13.	Test for supporting other protocol	√		
14.	Test for operation with DC power supply voltage variation	√		
15.	Test for internal Clock stability	√		
16.	Test for Noise level measurement	√		
17.	Test for Control Security and Safety for Control outputs	√		
18.	Test for functionality/parameters verification of CMRs & Heavy duty trip relays	√	√	√
19.	Test for data concentrator	√		
20.	Test for IED pass through	√		

21.	Test for SOE buffer & time data back up	√		
22.	Other functional tests as per technical specification requirements including features in support/ capability (for future)	√		
23.	Test for DC Power Supply of RTU	√		
24.	Test for compliance of standards for bought items viz. CMRs, Heavy duty trip relays, MFT, weather sensor etc.	√		
25.	Test for functionality/parameters for bought items viz. CMRs, Heavy duty trip relays, MFT, weather sensor etc.	√	√	
26.	Test for test tools		√	√
27.	Test for LDMS functioning		√	√
B	**EMI/EMC IMMUNITY TESTS FOR RTU**			
28.	Surge Immunity Test as per IEC 60870-2-1	√		
29.	Electrical Fast Transient Burst Test as per IEC-60870-2-1	√		
30.	Damped Oscillatory Wave Test as per IEC 60870-2-1	√		
31.	Electrostatic Discharge test as per IEC 60870-2-1	√		
32.	Radiated Electromagnetic Field Test as per IEC 60870-2-1	√		
33.	Damped Oscillatory magnetic Field Test as per IEC-60870-2-1	√		
34.	Power Frequency magnetic Field Test as per IEC-60870-2-1	√		
C	**INSULATION TEST FOR RTU**			
35.	Power frequency voltage withstand Test as per IEC 60870-2-1	√		
36.	1.2/50 µs Impulse voltage withstand Test as per IEC 60870-2-1	√		
37.	Insulation resistance test	√		
D	**ENVIRONMENTAL TEST FOR RTU**			
38.	Dry heat test as per IEC60068-2-2	√		
39.	Damp heat test as per IEC60068-2-3	√		
E	**Other test**			

40	Product cyber security compliance IEC 62443-4-2 /IEC62351 certificate of RTU from labs as per CEA order	√		

Table—2: RTU Type Test Requirements

Test Name	EUT Status	Test Level	Power Supply Points	I/O Points	Passing Criteria
Surge Immunity Test (Test 28)	ON	Level 3	2 kV	1 kV	2 kV
Electrical Fast Transient Burst Test (Test 29)	ON	Level 3	2 kV	-	1 kV
Damped Oscillatory Wave Test (Test 30)	ON	Level 3	2.5 kV	1 kV	2.5 kV
Electrostatic Discharge (Test 31)	ON	Level 3	+/- 6 kV in Contact discharge mode or +/- 8 kV in Air discharge mode	-	A
Radiated Electromagnetic Field (Test 32)	ON	Level 3	10 V/m electric field strength	-	A
Damped Oscillatory Magnetic Field test (Test 33)	ON	Level 3	30 A/m at 1MHz of magnetic field strength	-	A
Power frequency magnetic field (Test 34)	ON	Level 3	30 A/m of magnetic field strength (Continuous duration sine wave)	-	A
Power frequency voltage withstand (Test 35)	OFF	-	1 kV rms for 1 minute	-	No breakdown or flashover shall occur
1.2/50µs impulse voltage withstand (Test 36)	OFF	-	2 kVp	-	No breakdown or flashover shall occur
Insulation Resistance Test (Test 37)	OFF	-	Measure Insulation resistance using 500 V DC Megger before & after Power Freq & Impulse voltage withstand tests	-	As per manufacturer standard
Dry heat test (Test 38)	ON	-	Continuous operation at 55°C for 16hrs	-	0
Damp heat test (Test 39)	ON	-	at 95% RH and 40°C	-	0

-----End of Chapter 11-----

CHAPTER 12: SUPPORT SERVICES AND TRAINING

This chapter describes general requirements that apply to all training courses. The contractor shall submit the training proposal along with the bid. The training content, schedule and location shall be finalized during project execution.

12.0 General

a) Training will be conducted by Contractors personnel, who are experienced instructors and speak understandable English.

b) All necessary training materials shall be provided by the Contractor. Each trainee shall receive individual copies of all technical manuals and all other documents used for training.

c) Class materials, including the documents sent before the training courses as well as class handouts, shall become the property of owner. NEA reserves the right to copy such materials, but for in-house training and use only.

d) Hands-on training shall utilize equipment similar to that being supplied under the contract.

e) For all training courses, the travel and per-diem expenses will be borne by the owner.

f) The Contractor shall quote training prices under project management cost. & shall be included in the bid

g) The schedule, location, and detailed contents of each course will be finalized during employer and contractor discussions shortly after placement of the award. The Consultant/Employer shall review and approve the contents of the overview training prior to the start of the training.

12.1 Training Course Requirements

Employer's training course requirements are described below in terms of the contents of each course to be provided. Training shall be provided on actual database for the application software course and the associate training courses.

12.1.1 Database, Display Building & Report generation Course

The database and display building course shall be the first course to be given in the overall training sequence. It shall be a hands-on course using the hardware and software to be supplied by the contractor. The course shall be designed to train owner personnel in how to develop the databases, displays, reports, and logs for the offered system.

Course objectives shall include:

a) How to set up a database & display development system

b) How to identify database fields, entries, records, tables, and contents

c) How to structure RTU table definitions

d) How to build tables, arrays, and report formats and displays.

e) How to perform database maintenance

f) How to generate the database from source information

g) How to maintain symbol libraries, display color groups, and display string lists.

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.

12.1.2 Computer System Hardware & Software Course

The computer system hardware & Software course shall be offered, at the system level only. The training course shall be designed to give owner hardware & software personnel sufficient knowledge of the overall design and operation of the system so that they can correct obvious problems, configure the hardware, perform preventive maintenance, run diagnostic programs. The following subjects shall be covered:

a. **System Hardware Overview:** Configuration of the system hardware.
b. **Operating System:** Including the user aspects of the operating system, such as program loading and integrating procedures; scheduling, management service, and NEA functions; and system expansion techniques and procedures
c. **System Initialization and Fail over:** Including design, theory of operation, and practice
d. **Equipment Maintenance:** Basic theory of operation, maintenance techniques and diagnostic procedures for each element of the computer system, e.g., processors, auxiliary memories, LANs, routers and printers. Configuration of all the hardware equipments.
e. **Diagnostics:** Including the execution of diagnostic procedures and the interpretation of diagnostic outputs,
f. **System Expansion**: Techniques and procedures to expand and add equipment such as loggers, monitors, and communication channels.
g. **System Maintenance:** Theory of operation and maintenance of the hardware configuration, fail over of redundant hardware etc.
h. **Operational Training:** Practical training on preventive and corrective maintenance of all equipment, including use of testing tools.

12.1.3 Application Software Course

The Contractor shall provide training on Application software courses covering all applications other than those already covered above. The training shall include:

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

b. Application Functions: Overview of Functional capabilities, design, and algorithms. Associated maintenance and expansion techniques.

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

d. Software Documentation: Orientation in the organization and use of system software and Application software documentation.

e. Hands-on Training: shall be provided with allocated computer time for trainee performance of unstructured exercises and with the course instructor available for assistance as necessary.

12.1.4 RTU Course

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

a. Theory of operation of all RTU functions

b. Operational procedures for various modes of operation, including diagnostic tests and interpretation of the associated test results

c. Implementing and maintaining multiple communication ports

d. Converting an RTU from one protocol to a different protocol

e. Demonstration of complete RTU 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 problems

f. Disconnection and replacement of all RTU equipment, including all modules within the RTU

12.1.5 Operator Training Course

This training course shall provide training to Owner's operators on SCADA System so that operators can manage the system effectively.

The training shall include:

(a) **System Overview:** Configuration of the system, a functional overview, and an overview of system capabilities and performance.

(b) **General Operating Procedures:** Hierarchical structure of displays, display capabilities and features, user procedures, log-on and user access restrictions, and error messages.

(c) **System Applications:** Theory of operation, capabilities, and operating procedures for each application function.

(d) **Handling of Equipment:** Minor maintenance operations, such as removal of stuck paper in printers etc., which do not require spares/specialized skills.

(e) **Operator Documentation:** Orientation in the organization and application of all user documentation for Operator and verification of the information contained therein.

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. In addition, there shall be training for Instructor to use DTS & NSRC .

12.1.6 SCADA , networking, power supply related Training:

The training shall focus on critical aspects associated with installation, testing & commissioning , operation , maintenance of SCADA & Leased network equipment & Auxiliary power supply related training however, responsibility of service provider & contractor who has signed SLA with NEA, but required level of knowledge for troubleshooting, up keeping the equipment will be required**.** This shall include the state-of-the art techniques employed in laying, splicing & testing of fiber optic cable & terminal equipments etc. The owner's personnel shall be trained in such a way that the basic maintenance of terminal equipments & cable etc. can be carried out effectively.

-----End of Chapter 12-----

CHAPTER 13: SUPPORT SERVICES- FMS and SLA's

This chapter describes general requirements describes the project's spares and maintenance requirements.

13.0 Introduction

The Contractor shall be required to provide the services through Facility Management Service provider so as to manage SCADA system for Substation of NEA as applicable including all equipments, installations including hardware, software & networks installed & commissioned by Contractor for the NEA in order that they meet the availability requirement as specified in the document.

System Management Services shall be provided by the FMS Contractor, i.e., SI, to ensure maximum uptime and optimal performance levels of the installed SCADA systems. The FMS Contractor is expected to deliver services with performance levels meeting or exceeding those specified in the Service Level Agreement (SLA) agreed upon between NEA and the Contractor.

To achieve the desired Service Levels, the Contractor may need to interact, coordinate and collaborate with the other Service Providers as required. The Contractor will act as the Single Point of Contact for all issues relating to the Service Levels. The Contractor will have the responsibility to deal with the other vendors (during warranty period) /other vendors as selected by NEA (after warranty period) as the case maybe, to provide the services at agreed service levels. However, the prime responsibility of providing desired services shall be that of lead Contractor during warranty period. The role of FMS Contractor shall start immediately after systems are installed, commissioned and handed over to the owner after Operational acceptance of the SCADA System.

13.1 Scope of Work (FMS)

The Scope of Work shall include the software and hardware maintenance support to be provided by the Contractor in respect of the system supplied under this project for 4 years Facility Management Services (FMS) period along with Supervision & Operationalizing 4 year warranty serving entire FMS period of the SCADA System after the Operational Acceptance of the SCADA System.

The maintenance of the SCADA System under FMS period shall be comprehensive, as set forth herein, in nature and would broadly include but not be limited to diagnosis and rectification of the hardware and software failures. The Scope also includes:

- Co-ordination with equipment supplier for Repair/ replacement of defective equipment
- Configuration of the replaced hardware/software, periodic routine checking as part of preventive maintenance program (as described in further detail in this document) which would include checking of functionality of hardware and software,
- Services to maintain, bring up any or all SCADA systems upon its failure and to restore

- the functioning of SCADA system including Control Centers and field equipment, communication under the scope etc. .
- Database sizing and CFE card addition for new RTUs
- Creation / modification /deletion of database , displays , reports etc.

- All Software modules under the SCADA System and the associated Hardware supplied under this project.
- Communication & auxiliary power supply

Contractor shall also carry out routine works like database building/ modification, report creation/ modification, addition of analog, status points, control points and testing from field and other such day-to-day operational activity in presence, knowledge and concurrence of NEA representatives. The information of modifications shall be documented by contractor and NEA. Further, supply of quantity of RTUs beyond mentioned in the contract shall be responsibility of NEA. In case RTUs and associated components are added for further growth in the network during FMS period and are part of supply by SI only (as per same unit rate of the contract for implementation and **4 Years** of FMS period after operational acceptance , then SI shall also responsible erection , commissioning of the same). Otherwise, the responsibility of SI will be limited to control center activities data base population, mimic, report generation /modification including end to end testing.

The Scope does not include management of physical security for access to the said facilities, the following facilities will be provided at the start of contract to FMS Contractor by NEA for carrying out the FMS responsibilities:

- Sufficient Operators for dispatch control (However, SI shall provide adequate training to NEA operators for supervision and control and handhold for at least one initial year during FMS for the same. In any case, operations shall be made by NEA personnel or agency hired for operations by NEA only).
- Appropriately secured lockable storage/setup area
- Sufficient Sitting/office space in neat & clean environment
- PC (other communication facilities like P&T telephone & internet facility are to be arranged by FMS Contractor)

NEA shall provide all logistic support including access, work permits / shutdowns, Air-conditioning, raw power supply at control centers, furniture and other interface requirements on field of components which are not in the scope of contractor.

13.1.1 Hours of cover

The Contractor's on-site support standard hours of service the timings for Emergency Software Support would be 24 hours a day, 7 days a week throughout the year (i . e .24x365). Adequacy of Manpower deployment is the responsibility of SI to maintain SLA . However, per contract there shall be minimum one FMS project manager , One engineer each for hardware , software, network communication of Control centre , one engineer per substation for RTU, Communication shall be deployed. One certified cyber security engineer per contract/ control centre . The quantity is minimum, however S I to evaluate and deploy more manpower if required to meet SLA at no additional cost to NEA. The support personnel so deployed shall be qualified personnel having experience in the delivered SCADA system. The Contractor shall submit the CV's of all such personnel to NEA .The manpower specified is minimum, however, contractor shall ensure sufficiency of manpower to meet SLA during FMS period.
The minimum manpower stated above is required to consideration of FMS calculation. The Contractor shall be responsible for 24*7*365 management of all the systems as per scope of work with services rendered at least as per Service Level Agreement between NEA & Contractor.

13.1.2 Essence of the Agreement

The essence of the Agreement (to be entered) is to provide FMS for the designated hardware and software, with the goal of meeting the Availability as set forth herein and to provide system tuning and configuration to accommodate a growing system.

13.1.2.1 Service Delivery Management

FMS Contractor shall provide detailed description for service delivery management for the complete project including transition plan and deliverables and project management methodology.

a) Project Management

During FMS, a Project Manager for NEA, who will provide the management interface facility and has the responsibility for managing the complete service delivery during the contractual arrangement between NEA and the FMS Contractor. Project Manager will be responsible for preparation and delivery of all monthly/weekly reports as well as all invoicing relating to the service being delivered. Project Manager's responsibilities should essentially cover the following:

- Overall responsibility for delivery of the Statement of Work/s (SOW) and Meeting Service Level Agreement (SLA).
- Act as a primary interface to NEA for all matters that can affect the baseline, schedule and cost of the services project.
- Maintain project communications through NEA's Project Leader.
- Provide strategic and tactical recommendations in relation to technology related issues
- Provide escalation to Contractor's senior management if required
- Resolve deviations from the phased project plan. Conduct regularly scheduled project status meetings.
- Review and administer the Project Change Control Procedure with NEA
- Identify and resolve problems and issues together with NEA Project Leader. Responsible for preparation and delivery of all monthly reports as well as all invoicing relating to the services being delivered

b) Install, Moves, Adds, Changes (IMAC) Services

This Service provides for the scheduling and performance of install, move, adds, and change activities for Hardware and Software. Definitions of these components are as follows:

i. **Install:** Installation of desktop machines/workstations, servers, peripheral equipment, and network-attached peripheral equipment, which form part of the SCADA System supplied under the contract (new equipment needs to be procured by the NEA or due to growth of network).

ii. **Move:** Movement of desktop machines/workstations, servers, peripheral equipment, and network-attached peripheral equipment.

iii. **Add:** Installation of additional hardware /software after initial delivery

iv. **Change:** Upgrade to or modification of existing hardware or software on desktop/workstations and servers etc.

Requests for IMAC shall be prepared by FMS Contractor depending on system requirements & shall be approved by NEA. NEA shall formulate guidelines for IMAC & communicate it to

FMS Contractor. All procurement shall be done by NEA other than replacement of faulty items as per warranty /SLA under FMS period of the said item. Any item consumed during warranty period from SI supplied spares to NEA, shall be replenished by SI.

c) Contractor Management Services

As part of this activity, for efficient and effective warranty implementation, the FMS Contractor's team will:

1. Manage the vendors for escalations on support
2. Logging calls and co-ordination with Contractors
3. Contractor SLA tracking
4. Management of assets sent for repair
5. Maintain database of the various vendors with details like contact person, Tel. Nos., response time and resolution time commitments. Log calls with vendors, Coordinate and follow up with the vendors and get the necessary items exchanged.
6. Analyze the performance of the Contractors periodically (Quarterly basis)
7. Provide MIS to NEA regarding tenure of completion of warranty/AMC with outside vendors for software, hardware & networks maintenance in order that NEA may take necessary action for renewal of warranty/AMC. FMS Contractor shall also provide MIS regarding performance of said Contractors during existing warranty/AMC.
8. Since during initial 3 years, warranty is in scope of OEM vendors there will be no AMC for SCADA system. During such period, FMS Contractor has to interact with such vendors for maintenance services and spares. After warranty period, if required NEA can award the suitable AMC and FMS Contractor has to interact with Contractors as selected by NEA for providing AMC for the said system on mutually agreed terms & conditions.
9. The faulty hardware /software may be replaced from available spares of NEA to minimizing downtime time. However, in such case the same be replenished to NEA by SI within a month.

d) FMS Contractor's (SI) Other Responsibilities

1. Provide a single-point-of-contact for responding to NEA's queries or accepting its problem management requests. **FMS Contractor's** specialist will respond to NEA's initial request within agreed service level objectives set forth.
2. Monitor availability & escalate to service provider and Notify NEA for communication failures.
3. Review the service levels of the service provider (as per pre-defined schedules on SLA performance) along with NEA.
4. Provide network availability incident reports severity wise to NEA in a format mutually agreed.
5. Provide SLA performance management report of the Service Provider.
6. **Fault Detection and Notification:** The Contractor shall diagnose problems that could arise

as part of the LAN/WAN network. These include connectivity problems due to failures in communication transport links, routing configuration points, or from software bugs etc.

7. **Fault Isolation and Resolution:** All faults that have been identified need to be isolated and rectified appropriately. The resolution measures undertaken by the Contractor and results produced accordingly shall be documented in the report.
8. **Carrier Coordination:** Carrier Coordination implies providing a single point of contact to resolve network related problems involving carrier circuits, whether equipment or circuit related. When a problem is diagnosed because of a WAN circuit, the Contractor must coordinate with the corresponding carrier to test and restore the circuit. The Contractor must take the responsibility and ensure that the problem is resolved.
9. **Hardware/Software Maintenance and Monitoring:** This would include problem determination, configuration issues, and hardware and software fault reporting and resolution. All such issues would need to be recorded and rectified.
10. **24x7 Network Monitoring and reporting:** The Contractor shall monitor the network on a continuous basis using the NMS and submit reports on a monthly basis with instances from the NMS system. System performance is to be monitored independently by the Contractor and a monthly report mentioning Service up time etc. is to be submitted to NEA. The report shall include:
    - Network configuration changes
    - Network Performance Management including bandwidth availability and Bandwidth utilization
    - Network uptime
    - Link uptime
    - Network equipment health check report
    - Resource utilization and Faults in network
    - Link wise Latency report (both one way and round trip) times.
11. Historical reporting for generation of on-demand and scheduled reports of Business Service related metrics with capabilities for customization of the report presentation.
12. Generate SLA violation alarms to notify whenever an agreement is violated or is in danger of being violated.
13. Any other reports/format other than the above mentioned reports required by NEA

e) Backup/Restore management

FMS Contractor will perform backup and restore management in accordance with mutually MS Contractor shall ensure**:**

1. Backup and restore of data in accordance to defined process / procedure.
2. 24 x 7 support for database restoration requests
3. Maintenance and Upgrade of infrastructure and/or software as and when needed.
4. Performance analysis of infrastructure and rework of backup schedule for optimum utilization.
5. Generation and publishing of backup reports periodically.

6. Maintaining inventory of onsite tapes.
7. Forecasting tape requirements for backup.
8. Ensuring failed backups are restarted and completed successfully within the backup cycle.
9. Monitor and enhance the performance of scheduled backups
10. Real-time monitoring, log maintenance and reporting of backup status on a regular basis.
11. Management of storage environment to maintain performance at optimum levels.
12. Periodic Restoration Testing of the Backup
13. Periodic Browsing of the Backup Media
14. Management of the storage solution including, but not limited to, management of space, volume, RAID configuration, configuration and management of disk array etc.,
15. Interacting with Process Owners in developing / maintaining Backup & Restoration Policies / Procedures to provide MIS reports as per agreement

f) Restoration of Control Centre in case of Failure

The FMS Contractor shall ensure that all the relevant data is transferred from control center at regular frequency to Data Recovery Centre (DR) which is required for restoration of Control Centre in case of complete failure of Control center. FMS Contractor shall carry out system build in order to build the SCADA system at Control center from scratch from software licenses of control center data stored at backup control centre . However, in such condition where damage of control center is not attributed to SI , the development will be done on hardware procured by NEA . In case the damage is attributed due to SI , SI shall be liable provide control center hardware.

g) Performance Monitoring & Reporting

- Regularly monitor and maintain a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, Central Storage etc.
- Regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems, databases, applications etc. The system administrators shall also ensure that the logs are backed up and truncated at regular intervals.
- The administrators shall undertake actions in accordance with the results of the log analysis to ensure that the bottlenecks in the infrastructure are identified and fine-tuning is done for optimal performance

Reporting to NEA for all system performance monitoring % of availability of RTU & it's COMMUNICATION in a month (Minimum 99%). For % of availability of RTU & Analog status & control points (Minimum of total count end to end tested/ total count and for its communication total no of hours , the link was up / total no of hours in a given period) status to be derived from trend table and failure reporting of control command execution event , if any

- Cyber security audit by IT Security Certification empaneled agency of GoN on annual basis or interim audits in case of major change
- No cyber-attack or intrusion in SCADA system incident

The Contractor must adhere to well-defined processes and procedures to deliver consistent quality services throughout its contractual period. Any hardware/software to meet the requirements under this legacy system for integration must be provided by the Contractor. The Contractor is

expected to have the following system management controls in place:-

i) Availability Management

The Contractor must define the processes/procedures which ensure the service delivery as per the required SLAs or exceed it. It should cover various equipments such as all the servers, networks, switches, routers, Modems & other site specific services, and the critical services and their supporting hardware, and software components, as defined in scope of work. Industry standard SLA management tools should be deployed and shall have following essential features:

- Ability to create an escalation for an SLA.
- Ability to workflow the SLAs.
- Ability to create new action types, if needed.
- Ability to define sets of actions that are grouped together in a specific sequence. Ability to associate an escalation point with one or more actions through the
- action group.

ii) Performance Management

The recording, monitoring, measuring, analyzing, reporting, and forecasting of current levels, potential bottlenecks, and enhancements of performance characteristics for the services, networks, applications, system software, and equipment within the scope shall be required. System tuning and optimization is an inherent part of this contract. Where warranted, the Contractor will utilize capacity management data in combination with performance management data to identify ways to improve performance levels of the resources, extend their useful life, and request NEA to approve revisions/upgrades to the computing and communications hardware, software and other equipments such that higher levels of performance of the resources are obtained.

iii) Security Management

- The protection from unauthorized usage, detection of intrusions, reporting as required and proactive prevention actions are to be provided by the Contractor. No cyber-attack or intrusion in SCADA system incident
- Cyber security audit shall be carried out.

13.2 Support Services

13.2.1 Emergency Support

The severity levels are defined under clause 13.3 of this chapter. Emergency Support for Severity1 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 comprise of experienced technical staff that are skilled in troubleshooting SCADA systems. Severity 1 problems shall be reported by telephone for rapid response; target response times are defined in clause 13.5. The Contractor shall **submit the process details** to meet the above requirements along with the offer. For severity 1 problems, the key objective is to restore the system to an operational state as quickly as possible, including by a temporary work around. Resolution of the defect may be completed during standard hours.

Severity 2, 3, and 4 problems shall be reported by NEA through a call tracking system to be provided by the Contractor. The Emergency Support service goal is to meet the availability targets greater

than specified in this document (minimum 99% for Overall SCADA System). Resolution of problems may also be provided by an individual fix that will be installed by the Contractor at no extra cost to NEA.

13.2.2 Monitoring

The Contractor shall conduct the following monitoring, for the supplied SCADA System

13.2.2.1 Error Log Monitoring

To monitor the performance of SCADA system on a monthly basis, the Contractor shall review the following, analyze the results, and communicate to NEA:

- System logs for a selected day
- System history log
- Aggregate data collection
- Events Collection

During monitoring if any defect is found, the Contractor shall undertake corrective action for the same. The Contractor shall **submit the process details** to meet the above along with the offer

13.2.2.2 Resource Monitoring

Resource Monitoring services comprises checking the system's major node resources, gather log data, analyze results, and advise NEA on the appropriate actions to be taken and undertake any agreed upon actions. A tool will be created to continuously collect the following information:

- CPU loading (Peak and Average)
- System error log
- Disk utilization (Peak and Average)
- Operating system error reports
- LAN utilization (Peak and Average)
- Bandwidth utilization
- Memory utilization (Peak and Average)

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

13.2.3 Support for System expansion

New RTUs etc. per year are likely to be added to match the growing Power system. The services to be provided by the Contractor will include the Communication Front End (CFE) port/card addition/expansion, database resizing, interface addition in CFE and support for integration confirming to the IEC standards / existing application. This would not include the cost of equipments/card required for expansion**.**

13.3 Problem Severity Levels

The problems will be categorized as follows:

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 13.3.1).
Severity 2 – Serious	Degradation of services 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 13.3.1. Non-availability of Manpower at control center during working hours
Severity 3 – Minor	Any other system defect, failure, (As described at 13.3.1)
Severity 4 – General/Technical Help	Request for information, technical configuration assistance, "how to" guidance, and enhancement requests. (as described at 13.3.1)

The details of the system under different severity level are as below:-

13.3.1 Severity of the system under different Severity level.

a) Severity-1 (Urgent support)

This support is required when there is a complete system failure, 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 center. For example, loss of data to the operator due to any problem in SCADA system, ,Loss/failure of DR / Disaster recovery Centre, outages of both the CFEs attributable to any software/hardware related problem, outage of any important software functionality (on both the servers) which is required to disperse Distribution management & functions,

Failure of both GPS clock and time synchronization and outage of both routers, failure of both LAN system, outage of both main and backup servers of any system, firewall would be included under this category. The problem shall be attended by the Contractor at the earliest, within the response/Resolution time as specified in the Agreement on occurrence of incident. The Contractor shall take all steps to restore the SCADA functionality at the earliest to avoid data loss.

b) Severity-2

The support services not defined under Severity-1 are included under this category. Failure of one SCADA/FEP Server/ICCP server, failure of VPS , Stoppage of data collections for archiving, real time calculations, failure in Acquisition of SOE at the respective Control- Centre, outage of Real Time Network and distribution applications, and other applications are included in this category, Coverage under this severity would be outages that do not immediately

cause on feeder 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. Failure of any redundant system component affecting the critical redundancy like loss of any one Application Processor, Router, CFE would also be included in this category. Non-availability of Manpower at control center during working hours will also be covered under this category.

c) Severity-3 (Standard support)

The support services included under this category are when the outage or loss of functionality is neither an emergency nor a priority functionality as indicated in severity level 1 or 2 above. Problems like database reworking, failure of any one workstation, etc. would be covered under this Severity.

d) Severity-4 (General Technical Help)

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

13.4 Problem/Defect Reporting Procedure

The Contractor shall propose an appropriate problem/defect reporting procedure to meet the requirement of all severity level cases along with the offer.

13.5 Response and Resolution Time

This clause describes the target times within which the Contractor should respond to support requests for each category of severity. The *Initial Response Time* is defined time as the period between the initial receipt of the support request (through approved communications channels) and the acknowledgment of the Contractor. The *Action Resolution Time* is the period between the initial response/ incident concurrence and the Contractor delivering a solution. 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.

Except for Severity Level 1 & RTUs/ substation equipment , all hours and days specified are working hours only.

13.5.1 Emergency Support Response/Resolution Time

Severity	Initial Response Time	Action Resolution Time	Action
1	30 minutes	2 hours	An urgent or emergency situation requiring continuous attention from necessary support staff until system operation is restored – may be by workaround.
2	1 day	2 days	Attempt to find a solution acceptable to NEA as quickly as practical. Resolution time is dependent on reproducibility, ability to gather data, and NEA prioritization. Resolution may be by workaround.
3	2 days	5 days	Evaluation and action plan. Resolution time is Dependent on reproducibility, ability to gather data, and NEA prioritization. Resolution may be by workaround.
4	2 days	5 days	Report on the problem/query is to be furnished.

Downtime will be calculated time beyond response & resolution time

The Contractor shall submit the detailed format/procedure for all the activities such as Reporting time, Resolution time, Downtime etc. along with the offer.

13.6 Preventive Maintenance

The Contractor shall undertake preventive maintenance of all equipment/modules (i.e. Hardware & Software supplied under the SCADA System), under the scope of this contract, in accordance with this section. The Contractor will prepare the report as per periodicity defined below and submit the same to the Engineer-in-charge.

i) Activities shall include but not limited to:

a) Patch Management for OS and Application Software

b) Automatic update of Antivirus and firewall signatures on daily basis.

c) Average and peak usage of CPU, LAN, Memory and Disk –once every month

d) Monitoring of machine with reference to error reports and logs - once every week

e) Online diagnostics for servers and workstations - once every 3 months.

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

g) Physical hardware checks to ensure proper working of cooling fans etc.- once every 3 months.

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

i) Cleaning and blowing for removal of dust from Servers , Workstations, CFE

j) panels and RTUs etc.- once every 3 months.

ii) Exclusions:

a) Maintaining dust free / AC environment and protection from rodents and vermin is the responsibility of NEA.

b) Regular cleaning of computer furniture and surroundings is the responsibility of NEA.

c) Equipment shutdown during preventive maintenance shall be deemed as available.

13.7 Service Level Agreements (SCADA)

It is the endeavor of both the Contractor and NEA to maximize system availability to the extent possible. The Contractor shall provide guaranteed availability for various types of Severity levels as specified in clause 13.3 above. The non-availability hours for availability calculation may be reckoned from the end of the allowed Action Resolution time. A standardized register/ log on system shall be maintained at each site containing full details of each outages, actions taken by NEA to correct the problem, applicable Severity level, time of reporting to the Contractor/SI support engineer/support centers pursuant to the appropriate methods in the Agreement, allowed Response time as per the Response times defined in clause 13.5, actual Resolution time, and signature of NEA's Engineer-in-charge as well as the SI's/Contractor's support engineer of the site. Duration of outages over and above the Action Resolution time 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 accomplished by a work around, and such 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 duet unrelated cause would be counted separately

13.7.1 Availability computation for SCADA System

Availability would be on per quarterly basis. The formula to be used for availability computation would be as under:

$$\text{Availability per quarter (per site)} = \frac{THQ - (S1 \times 0.6 + S2 \times 0.3 + S3 \times 0.1) \times 100\%}{THQ}$$

- Where THQ is total hours in the quarter
- S1 is the total non-available hours in Severity Level-1
- S2 is the total non-available hours in Severity Level-2
- S3 is the total non-available hours in Severity Level -3

In case of cyber-attack incident which is not neutralized by cyber security and affected the system, the availability shall be considered nil.

14.7.2 Payment of maintenance charges (based on SCADA System availability)

In the event of availability below a certain level, the maintenance charges would be proportionately reduced as follows. The non-availability will be considered if system is non available beyond reporting/response + resolution time :

Penalty For overall system availability (S)

Availability per Quarter	**Deduction as % of the apportioned price of total FMS for SCADA portion of the contract applicable for the site**
> 99%	NIL
Less than 99%	Deduction of 2.5 % of the apportioned price on each 1% non-availability below 99% and upto 95% and deduction of 4 % of the apportioned price on each 1% non-availability upto 90% & 100% deduction below 90%

While calculating Availability following shall be considered:

The Overall SCADA System shall be considered as available if

a) All SCADA applications are available
b) Requests from available Operator Consoles & VPS are processed
c) Information Storage and Retrieval applications are available
d) Data exchange with other system is available
e) One of the redundant hardware is available so that all the SCADA applications are functional to ensure the design & performance requirement as envisaged in the MTS
f) DC/DR data exchange and synch at defined periodicity
g) Performance calculation report/ dashboard for FMS is available and shall be system generated

Further, non-availability of legacy systems shall not be considered for calculating Overall SCADA System Availability. However, data availability from legacy to be ensured.

Further, the non-availability of following non-critical functions shall not be considered for calculations of SCADA System availability, however these functions should be available for 98% of the time.

a. Database modification and generation
b. Display modification and generation
c. Report modification and creation
d. DTS

For individual critical hardware & functions (C)

Availability per quarter	**Deduction as % of the apportioned price of total FMS for SCADA- for SCADA portion of the contract applicable for that site and all critical hardware/ redundant hardware**
≥ 99%	NIL

Less than 99%	Deduction of 2.5 % of the apportioned price on each 1% non-availability below 99% and up to 95% and deduction of 4% of the apportioned price on each 1% non-availability upto 90% & 100% deduction below 90%

for individual hardware or non-critical functions (N)

Availability per quarter	**Deduction as % of the apportioned price of total FMS for SCADA portion of the contract applicable for the site**
≥ 95%	NIL
Less than 95%	Deduction of 2.5 % of the apportioned price on each 1% non-availability below 95% and up to 90% and deduction of 5% of the apportioned price on each 1% non-availability up to 85% & 100% deduction below 85%

Critical function /hardware:

SCADA functions, Defined reports incl Servers, LAN, WAN, VPS , GPS time synch , Mass storage Operator workstation , CFE/FEP and redundant hardware /software etc and associated communication and auxiliary power supply. For In dividual critical hardware/software, response/report and resolution time shall be as per severity 1 if both main and standby failed, and shall be per severity 2 if one of main or standby system , VPS, till one workstation at least for project area is available

Non-Critical function /hardware:

Response/report and resolution time shall be as per severity 3, if Database & mimic development , DTS , and non -redundant hardware /software etc & associated communication and auxiliary power supply is not available

CALCULATION OF EACH CRITICAL HARDWARE /SOFTWARE FOR SITE FOR QUARTERLY FMS =

= % C FOR CRITICAL INDIVIDUAL HW/ SW = (Total Hours up OR running / total Hours in quarter)*100

=N % FOR NON-CRITICAL INDIVIDUAL HW/ SW

% N FOR NON-CRITICAL INDIVIDUAL HW/ SW = (Total Hours up OR running /total hours in quarter)*100

FMS for items , if applicable at NSRC shall be excluded from SLA calculation and to be calculated separately for NSR.

For RTUs

Availability per quarter	Deduction as % of the apportioned price of total FMS for apportioned portion of RTU and associated communication and power supply applicable
≥ 99%	NIL
Less than 99%	Deduction of 1 % of the apportioned price on each 1% non-availability below 99% and upto 95% and below 95% & up to 90% and deduction of 2% of the apportioned price on each 3% non- availability below 90% up to 80% & 100%deduction below 80% . Availability of RTU, is determined by up OR functional status of RTU in hrs. / total no of hours in quarter & the link was up / total no of hours in a quarter and data availability of status and analog and control points tested for end to end upto beginning of that quarter whichever is lower . The measurement of data acquisition and control shall be assessed through at each 15 min integrity cycle/ or as per recorded trend which ever minimum 99% points shall be reported and controllable for

Response/report and resolution time shall be as per severity 2 in case of failure , = % R in Qtr = Min ((RTU up in Hrs / total Hrs), (Link up in Hrs / Total Hrs), (No of points with good telemetry code captured / total number of points end to end tested) *100%

For Manpower shortage during FMS:

% shortage of manpower during FMS by bidder shall be calculated for each quarter and manpower deployment less than 30% in any quarter will lead to 75% deduction in FMS amount of that quarter (example: if 18 persons are deployed instead of 20 then there will be 10% shortfall of manpower & 2 % amount admissible for FMS in that quarter will be deducted. from payment of quarterly SLA). The amount deduction on shortfall of manpower in FMS i.e. 30% or more will attract deduction of 2% amount per 10% deduction in manpower deployment during FMS.

Penalty Applicable during the Implementation Period:

The rollout of SCADA System including all the applications/supporting system in all the project areas has to be completed by the SI as mentioned in RFP or as per the agreed roll out plan. Any delay in the SCADA System roll-out will attract penalty for every month of delay subjected to maximum penalty of 10%. It will be levied for the duration equivalent to number of weeks (months) delayed which shall be deducted from subsequent months based on the milestone payments

Sl. No.	Project Phases	Timelines	Penalty for Delay
1.	Overall SCADA System and Field Infrastructure Installation, end to end testing & Commissioning	T + 36 months	0.5% per month or part there of maximum up to 7% of the total cost quoted for SCADA system Implementation

In case, the System Integrator is unable to implement the any part of the scope of work within the given timelines and project implementation duration is extended beyond the period of 3 years. In such case, the NEA reserves the right to get the remaining part of project work completed from other agencies at the cost of the SI.

13.8 The SI's / Contractor's Obligations

To optimize and improve the response of the system, the Contractor may re-install the program modules after making the NEA 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, patches, or arising out of a necessity to fix FPRs, would be done by the Contractor at no extra cost to NEA. Also, any software updates/upgrades released till the completion of warranty period /FMS shall be provided and installed & commissioned free of cost as per instructions from NEA.

The Contractor shall ensure that all components (Hardware & Software) covered under minimum 4 years or comprehensive on-site warranty are maintained in good working condition and in case of any defect , timely replacement/repair shall be carried out so as to meet the availability requirements specified herein. The entire FMS period shall be covered. If not, the same warranty shall be extended by SI.

The Contractor will submit FSR (Field Service Report) and the steps taken to solve the problem, along with details of code changes.

13.9 Responsibilities of NEA

a) NEA will ensure the availability of competent staff appropriately trained in the administration and use of existing SCADA systems for proper operation of the system.

b) NEA shall ensure that proper Environmental conditions are maintained for the system.

c) NEA shall ensure that the System is kept and operated in a proper and prudent manner and only trained NEA employees (or persons under their supervision) are allowed to operate the system.

d) NEA shall provide access to the sites of installation for purposes of providing support Services.

e) NEA shall provide the Contractor with Office and storage space for their maintenance staff and spares. However , contractor shall be responsible for security of the items stored

13.10 Responsibility Matrix

The table in this clause provides a summary definition of the roles and responsibilities of the Contractor (A) and NEA (B).

Item	Task	NEA	Contractor
1.0	**PROBLEM IDENTIFICATION IIDENTIFICATION**		

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

3.0 ROUTINE SOFTWARE SUPPORT			
3.1	Build and maintain database, displays and reports		A
3.2	Perform system back-ups		A
3.3	Restore or reinstall software from back- ups		A
3.4	Monitor system logs (part of remote monitoring service)		A
3.5	Maintain system logs		A
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		A
4.3	Identify failed component, Replace failed components in online system using parts from spares inventory		A
4.4	Restore operation of repaired/replaced equipment		A
5.0	**HARDWARE SPARE PARTS**		
5.1	To keep inventory for SLA by SI		A
5.2	Provide appropriate facility for local storage of spares in case not available with SI but this is not obligation for NEA		A
5.3	Replenish local spares inventory		A
6.0	**INTEGRATION AND DATABASE WORK**		
6.1	CFE /RTU Card addition/Expansion field equipment		A
6.2	Database resizing, Mimic creation/ editing etc ,		A
6.3	Annual cyber security audit		A

The contractor shall be responsible for all the maintenance of the system till the operational acceptance. The consumables and spares wherever required for maintaining the system shall be provided by the contractor till operational acceptance of the system. The consumable items shall include but not be limited to (a) VPS lamps (b) printer paper (c) Printer toner, ink, ribbons and cartridges (d) Special cleaning material

-----End of Chapter 13-----

CHAPTER 14: PROJECT MANAGEMENT, QUALITY ASSURANCE AND DOCUMENTATION

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

14.0 Project Management

The Contractor shall assign a project manager with the authority to make commitments and decisions that are binding on the Contractor. SI will designate a project manager to coordinate all employer project activities. All communications between NEA 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.

Bidder shall submit the manpower deployment plan along with the bids, describing the key roles of each person.

14.1 Project Schedule

The project implementation schedule shall be not exceeding 24 months from the date of award. Based upon this schedule the bidder shall submit a preliminary implementation plan along with the bid. The detail project implementation schedule shall be submitted by the contractor after award for NEA's approval, which shall include at least the following activities:

a) Site Survey
b) Documents submission and approval schedule
c) Factory & Site Testing Schedule
d) Database development schedule
e) Hardware purchase & Manufacturing, Software development & integration schedule
f) Dispatch Schedule
g) Installation / commissioning schedule
h) Training schedule

The project schedule shall include the estimated period for completion of and its linkage with other activities.

14.2 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 NEA on a monthly basis, e.g., the 10th of each month. The progress report shall include all the completed, ongoing and scheduled activities.

14.3 Transmittals

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

14.4 Quality Assurance & Testing

All materials and parts of the system / sub-system to be supplied under the project shall be of current manufacture from a supplier regularly engaged in the production of such equipment.

14.4.1 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's plant, 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 Owner. Instructions and records for quality assurance shall be controlled and maintained at the system levels. The 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 acceptance by the Owner.

Such QA/QC program shall be outlined by the Contractor and shall be finally accepted by Owner after discussions before the award of Contract. A Quality Assurance Program of the Contractor shall generally cover but not be limited to the following:

a) The organization structure for the management and implementation of the proposed Quality Assurance Program.
b) Documentation control system.
c) Qualification data for key personnel.
d) 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.
e) System for shop manufacturing including process controls.
f) Control of non-conforming items and system for corrective action.
g) Control of calibration and testing of measuring and testing equipments.

h) Inspection and test procedure for manufacture.
i) System for indication and appraisal of inspection status.
j) System for quality audits.
k) System for authorizing release of manufactured product to NEA.
l) System for maintenance of records.
m) System for handling, storage and delivery.
n) A Quality Plan detailing out the specific quality control procedure adopted for
o) Controlling the quality characteristics of the product.

The Quality Plan shall be mutually discussed and approved by the NEA 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 effective Quality 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 NEA when actual quality deviates from that stated in the Work Statement.

The Contractor/SI shall be required to submit all the Quality Assurance Documents as stipulated in the Quality Plan at the time of NEA's inspection of equipment/materials.

NEA or his duly authorized representative reserves the right to carry out 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 , 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.

14.4.2 Inspection

The Contractor shall give the employer/Inspector two weeks in case of domestic supplies and six weeks in case of foreign supplies written notice of any material being ready for testing. Such tests shall be to the Contractor's account except for the expenses of the Inspector. The employer/Inspector,

unless witnessing of the tests is waived, will attend such tests on the scheduled date for which employer/Inspector has been so notified or on a mutually agreed alternative date. If employer/Inspector fails to attend the testing 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/Inspector 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 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 Sub-contractor's works, the employer/Inspector shall issue a certificate to this effect within fourteen (14) days after completion of tests but if the tests are not witnessed by the employer/Inspector, the certificate shall be issued within fourteen (14) days of receipt of the Contractor's Test Certificate by the Employer/Inspector. 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 with the Contract.

In cases where the Contract 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/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/Inspector or his authorized representative to accomplish testing.

The inspection by Employer 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 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 inspected and 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 the Contractor from the responsibility for furnishing material, software, and equipment to 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.

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 where equipment 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 the Contractor's hardware quality assurance standards, procedures, and records that are applicable to the facilities shall be provided to NEA.

14.4.3 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's 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 effectiveness 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 (c) Employer acknowledges in writing the successful completion of the test.

14.4.3.1 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.

14.4.3.2 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.

14.4.3.3 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.

14.4.3.4 Factory Test

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

a. Verification of all functional characteristics and requirements specified
b. 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 for the system 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.

14.4.3.5 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 in line to the requirements specified in the relevant sections of this volume.

14.5 Type Testing

The equipment being supplied shall conform to type tests as per technical specification and shall be subjected to routine tests in accordance with requirements stipulated under respective sections. The type test shall be conducted on the equipment if it is specifically mentioned in the relevant section, for other equipment the type test report shall be submitted. Employer reserves the right to witness any or all the type tests. The Contractor shall intimate the Employer the detailed program about the tests at least three (3) weeks in advance in case of domestic supplies& six (6) weeks in advance in case of foreign supplies.

The reports for all type tests as per technical specification shall be furnished by the Contractor along with equipment / material drawings. The type tests conducted earlier should have either been conducted in accredited laboratory (accredited based on ISO / IEC Guide 25 / 17025 or EN 45001 by the national accreditation body of the country where laboratory is located) or witnessed by the representative(s) of NEA. However, type test reports shall not more than five year old than the date of bid opening or validity of report by testing lab whichever is lower.

In the event of any discrepancy in the test reports i.e. any test report not acceptable due to any design / manufacturing changes or due to non-compliance with the requirement stipulated in the Technical Specification or the type test(s) not carried out, same shall be carried out without any additional cost implication to the Employer.

In case of failure during any type test, the Supplier at his own expenses shall modify the equipment and repeat all type tests successfully at his own cost and within the project time schedule.

Wherever, the make of the items is indicated in the technical specification, the type test reports are not required to be submitted for the makes, indicated in the specification. For the new makes (other than those indicated in the technical specification), type test reports as per

relevant standard shall be submitted for Employer's approval.

14.6 Documentation

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 manufacturing, system development, factory testing, site testing, training etc. The schedule for submission/approval of each document shall be finalized during the discussions before placement of the contract, this schedule shall be in line to overall project schedule.

Each document shall be identified by a Contractor document number, the employer document number, and the employer purchase order number. Where a document 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 approval by the Contractor's project manager. Each revision of a document shall highlight all changes made since the previous revision.

The contractor shall submit two copies of each document/drawing for employer's review and approval. After approval five sets 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 incorporated in the as-build drawing and required sets of the same shall be submitted to employer/owner. In addition to paper copies all the documents shall also be provided on electronic media in two copies. In case any documentation requirement is specified in the relevant chapters , the same shall apply for the equipment /system defined in that section. The contractor shall also supply five sets of User manuals/guides/O&M manuals/manufacturer's catalogues for all the hardware & software supplied under the contract which shall be in addition to the one set each 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.

a) System Description Documents (Overview)
b) Data Requirement sheets
c) Software Requirements Specification
d) Data base Documents
e) Drawings/Documents for manufacturing/Assembly of the equipment/system
f) Drawings/Documents for installation of the equipment/system at site
g) Software description/design documents for each software module
h) Testing Procedures and reports
i) Manuals for each equipment/hardware/test equipment
j) Bill of Quantities
k) Site Testing documents
l) Training documents
m) System Administrator Documents
n) User guide for Despatcher

However, all the above type of documents may not be required for each sub-system of the project e.g. item (n) above may not be required for auxiliary power supply system, therefore, 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. In regard to Data requirement sheets (DRS) for these will be duly filled in by the bidder & submitted along with the bid. During detailed engineering, contractor will be required to submit detailed DRS to include all technical parameters of the equipment to ensure that the offered equipment meets all the technical specification requirements

The Licensed Equipment manufacturers shall be able to manufacture, assemble, test, market and sell the product as per OEM type tested design under technology transfer agreement. The Licensed Equipment manufacturers should submit following documents:

a. Licensed Equipment manufacturers should furnish Technology Licensee certificate or agreement copy.
b. Licensed Equipment manufacturers should be able to furnish valid Type test certificate from OEM.
c. Tender specific Authorization letter backed by OEM shall be submitted at the time of tender.

------End of Chapter 14-----

CHAPTER 15

A) DESIGN PARAMETERS AND PERFORMANCE TABLES

The SCADA system shall be designed as per the technical parameters defined in the specification and the tables specified here.

The system shall be tested with the doubled present power system size (ultimate capacity) as defined in table 7& measure the various performance of the system as defined in the tables and technical specifications including peak and average load scenarios.

The auxiliary memory utilization , average CPU, RAM & LAN utilization parameters shall not exceed the limits as defined in table 8. This memory utilization includes the memory used for storage of data for the defined duration as specified in the various sections of technical specification.

The SCADA system shall be suitable for addition of at least double the operator workstations (in future) without requiring any up gradation of the servers.

The SCADA system design & performance parameters are defined in the following tables:

Table 1 – DESIGN PARAMETERS FOR SCADA FUNCTIONS

Note: The parameters which are not indicated in the tables & only mentioned elsewhere in the specification shall also be considered as design parameters

Chapter 2 /clause	Function Description	Design capacity	Execution rate
2.2.2 & Subclauses	**Data** Acquisition	**As per spec**	
	Status	By exception Integrity All status periodically 10 min (configurable cycle)	From RTU shall be reported by exception and shall be updated and displayed within 2 seconds.
	Analog	By exception Integrity All analog periodically 10 min(configurable cycle)	From RTU shall be reported by exception and shall be updated and displayed within 3 seconds.
		Max Time skew status	0.1sec at each location
		Max latency status	0.5sec .
		Max Time skew analog	1 sec at each location
		Max latency analog	1 sec

	Energy values	15-minute blocks shall be collected periodically from the RTU at scan rate of 15 minute/1 hour (configurable up to 24 hours	Update time and time skew as per analog data
2.2.3 & Subclauses	Time synchronization	RTUs	Every 15 minutes (user configurable from 5 minutes to 24 hrs.)
2.2.4 & Subclauses	Data exchange between SCADA control centers (DCC) & BCC center Min, max ,Avg	IT system If opted	As defined by NEA. As required for ISR function & data exchange
2.2.5 & Subclauses	Data Processing (status & analog) Min, max ,Avg		Each time the value is received For analog values
2.2.7	**Sequence-of-Events data**	1000 events circular buffer in the SCADA database	SOE retrieval Periodically (5 minutes) or by exception
2.2.9 & Subclauses	Supervisory Control		
	a) Control Inhibit Tag Type	4	a) (b) (c) On demand by Dispatcher function initiated
	b) Control inhibit Tags / device	4	
	c) Control Action Monitor		10 timer periods (1 to 60 sec) For all control points
	d) Control permissive		d) Each time supervisory control is requested
	e) Fail-soft capability	in the event of system crosses mark of peak loading requirements	graceful de-gradation of non –critical functions & also relaxing periodicity / update rate of display refresh & critical functions by 50%.

Table 2 – DESIGN PARAMETERS FOR ISR FUNCTIONS

Chapter 2 /clause	Function Description	Design capacity	Execution rate
2.3.1	**Circuit breaker status Table**	Real-time status of all Circuit breakers along with quality date & time of tripping and requirements as per specification	**Every time status** changes Daily tables online storage for 24 months
2.3.2	**Real-time Database Snapshot Tables**	a) All telemetered analog values and Calculated values for all tele- metered analog points (at least maxima & minima with associated time and average values). Energy values are not envisaged for storage in Data snapshot tables. b) All status values with time stamp	**Every 5 min Daily tables online storage for 24 months**
2.3.3	**Hourly Data tables**	Selected analog values along with their associated quality codes Selected status values along with their associated quality codes Results of hourly calculations for selected analog points (at least maxima & minima with associated time and average) along with their associated quality codes. In addition to above a separate hourly energy data table exclusively for energy values (Export and Import Active and reactive Energy values foreach feeder) shall be created in ISR along with their associated quality codes.	Hourly tables incl Missed and hourly data calculation on daily basis online storage for 24 months
2.3.4	**Daily Energy Data**		

		daily energy data table shall be generated for storage of daily energy values for 15 minute blocks / one hour blocks of a day feeder on daily basis along with quality codes.	daily basis online storage for 24 months
2.3.5	Load priority Table	Load priority table containing information such as breaker name, number of consumers connected to each Breaker and Load priority of each Breaker/Feeder	Monthly basis online storage for 24 months
2.3.6	SOE Data Table	All CBs, protection and alarm contacts shall be considered as SOE	Minimum daily 4 changes per SOE point may be considered Daily basis online storage for 24 months
2.3.7	User definable index table	Customized report	Daily basis online storage for 24 months
2.3.8	Average Time Restoration Table	avg time to report outage location, restoration of supply of feeder	Minimum daily 4 time restoration may be considered Monthly basis online storage for 24 months
2.3.9	Daily/Weekly Flash reports	Customized report for Management for daily basis	Daily basis online storage for 24 months
2.3.11	System Message Log Storage	System message log data storage shall be sized for up to 20,000 entries per month.	Monthly basis online storage for 24 months
2.4	Load Shed Application (LSA)	As per functional requirement	As per functional requirement in Spec
2.5	Common Disaster Replica Recovery		As per functional requirement in Spec
2.6	DATA recovery centre	network model of SCADA control center of each area shall be sent to back up control center periodically once a day & upon user request. All logs, data model etc. & necessary interfaces that are essential for complete system build up shall be stored at backup control center. All requisite data which is build the system from scratch shall be	As per functional requirement in Spec

		transferred to BCC. An alarm shall be generated & send to SCADA control center upon attaining user defined threshold e.g. 80% for storage at backup control center.	

Table 3 - MAINTENANCE ACTIVITIES

Action	Performance
Complete database regeneration	2 hours
Complete system software build, including operating system, applications, and	6 hours
Software build or all applications and databases	3 hours
Software build of a single application and	10 minutes
Installation of a single, new display including distribution to all consoles	60 seconds
Reinstallation of all displays	60 minutes
Perform an on-line update of a database parameter and propagation of the change to the source data	60 seconds

Table 4 - DESIGN PARAMETERS FOR USER INTERFACE

Chapter 3	Description	Minimum
	Windows	16
	Rooms	16
	Layers	8
	Variable per trend	8
	Alarm levels	8

Table 5 - CONFIGURATION CHARACTERSTICS &AVAILABILITY FUNCTIONS

Description	Max time in sec
Processor error detection	5
Other devices error detection	5
Processor switchover	30
Functional availability after switchover	10
ISR availability after switchover	120
Processor – Hot startup	Limited to switching time
Processor – Warm startup	600(10 min)
Processor- Cold startup except ISR /with ISR	900(15 min) / 1800(30min) ISR

Table 6- PERFORMANCE REQ

(a) USER INTERFACE REQUIREMENTS

At no time the SCADA system shall delay the acceptance of User request or lockout console operations due to the processing of application function

User interface requirements	**Response time(Peak loading)**
Requests for call-up of displays shall be acknowledged indication of request is being processed	Within 2 sec
Any real time display and application display (except DB displays) on workstation console, Complete display & values shall appear on screen	Within 3 sec after acknowledgement of request
Manual Data entry of the new value shall appear onscreen	Within 2 sec
Display update rate	Every 2 sec for at least
Panning of a world display from one end of screen to other end of screen in a continuous manner	Within 2sec
Supervisory control action shall be completed with displayed on the screen	Within (2sec + scan time +communication delay time +field device operation time)
Alarm and event response time	display within 1 sec of receipt in SCADA System
Alarm and event acknowledgement	With in 2 sec
Requests for printing of displays shall be acknowledged an indication of request is being processed	Within 2 sec

Requests for generation of reports shall be acknowledged an indication of request is being processed	Within 2 sec

(b) UTILISATION

(Considering double the present power system size)

Name	Average Utilization	Comments
PROCESSOR	30%	Normal loading
Servers	50%	Peak loading
LOCAL AREA NETWORKS	15%	Normal loading
	40%	Peak loading
Main memory utilization (avg)	50%	Normal loading
	67%	Peak loading
Auxiliary memory utilization	50%	

Table 7- ACTIVITIES FOR NORMAL AND PEAK LEVEL OF LOADING
(Considering double the present power system size)

(1) NORMAL LEVEL OF ACTIVITY

The normal level of activity shall simulate system activities spread over one hour period. During the testing, the response times and the average utilizations shall not exceed the specified values. The following conditions define normal level of system activity to generate the normal loading scenario. Test simulation shall be done using software tool to generate this loading within 1 hr. Staggering of loads during the test duration of I hour is permitted.

I) All RTU data shall be scanned and processed

II) All data exchange with other systems shall occur as specified in the specification.

III) All periodic functions shall be executed at the rates defined in tables

IV) The following SCADA functions shall be executed on-demand:

Function	**Number of demand executions**
Substation topology processor	50 state changes
Sequence-of-Events data	50 SOE points reported

V) Alarms (2 X no. of RTUs) per hour shall be generated. Each alarm shall be acknowledged individually within 5 seconds.

VI) Events (2 X no. of RTUs) per hour shall be generated.

VII) 1% analog of total analog/ 5sec measurements of total analog point count changes as per IEEEC37.1

VIII) One complete run of on-line diagnostics shall be performed on all computers

IX) Communications channel monitoring shall be performed

Display Selection	**30 per operator workstation & VPS**
Supervisory control actions	2 per RTU & 1 per 50 RTUs
Display Updates	Each operator workstation shall display 3 updating and 1 non- updating display window per monitor. This also includes VPS. **Updating displays:** - alarm summary list - world display containing a S/S SLD - Network display **Non-updating displays:** - SCADA System Display
Data Entry	5 data entry actions from any single display
Display Trending	8 display trends, each trending 4 variables
Reports	Prepare and printing of 5 reports

The following maintenance activities shall be performed:

Function	Task
On-Line Database Editing	Modify 20 data points in each of the 5 RTUs
Display Generator and Management	Modify one single-line diagram one tabular display

2) PEAK LEVEL OFACTIVITY

The peak level of activity is an addition to the average level of activity described in (A) NORMAL LEVEL OF ACTIVITY above. The peak level of activity shall be applied for a five minute period. During the next ten minutes, only the normal level of system activity shall be applied. This test shall be repeated for four consecutive fifteen minute periods, fora total peak level test time of one hour. The five-minute peak loading period shall coincide with SCADA system period where all periodic software is scheduled for execution and at least one five minute period shall span an hour boundary to consider the scheduled hourly periodic activities. There shall be no restrictions on the period when the five-minute peak can occur.

(a) As per IEEE C37.1
   i. 15 % of status of total status points/ 5sec measurements
   ii. 40% analog of total analog measurements /5sec
   50% of the alarms shall be acknowledged within the five-minute period (automatic acknowledgement is unacceptable).

(b) Display Requests
   6 display requests per minute per console

(c) Supervisory Control
   Total 1 per RTU & 1 per 10 RTUs in 5 Minute period of peak loading cycles

(d) Reports Prepare : 5 reports.

The above are indicative, NEA may align with their Standard operating procedure after the award of contract.

---End of SCADA PERFORMANCE TABLES---

Table 8 BOQ (Bill of Material: SCADA)

The BOQ shall be composite along with separate for break up for each Control center (SCADA)

PART A: SCADA BOQ (DCC Hardware)

Item No.	DCC-Hardware	Estimated	
		Unit	Quantity
1.	SCADA Server	No.	2
2.	FEP server	No.	2
3.	ICCP server	No.	2
4.	ISR Server	No.	2
5.	Historian server	No.	2
6.	NMS server	No.	1
7.	DTS server	No.	1
8.	Web server with load balancing	No.	2
9.	Integration Server	No.	1
10.	PMS and AV server (Patch Management & Antivirus)	No.	1
11.	**Other Active Devices**		
a	Configuration and Developmental server(C&DS)	No.	1
b	QAS server (Quality Assurance server) for patch testing	No.	1
c	Active Directory server	No.	1
d	SMS gateway	No.	1
e	Developmental console with one TFT	No.	2
f	DTS/Workstation Console with dual TFTs	No.	2
13	**Storage & Backup Devices**		
a	Network Attached Storage (NAS) or SAN Storage Array with **minimum 20TB usable capacity** (configured in RAID 6 or RAID-TP) to ensure retention of 7 years of historical data and 2 years of online alarms/events for the Ultimate system sizing. The system shall support Active-Active controllers and AI-driven management	No.	1
b	LTO Tape Drive or Disk-based Backup Solution.	No.	1
14	**Switches**		
a	Layer II switch (SCADA LAN and ISR LAN)	No.	2
b	Layer II switch (Configuration and Developmental system LAN and QAS LAN)	No.	2
c	Layer II switch (FEP) - 24 ports	No.	2
d	Layer II switch (ICCP) - 24 ports	No.	2
15	**Routers**		
a	Industrial Services Router for interfacing IT systems, DRC and Transmission Control Centers, supporting MPLS/VPN.	No.	2
16	**Security system (DMZ)**		
a	Firewall including IDS/IPS, Web filtering, VPN	No.	4
b	Layer II switch	No.	4
c	Router cum firewall for ICCP	No.	2
d	Router cum firewall for FEP	No.	2
17	**Other Active Devices**		

a	GPS Time synchronisation system	Set	2
b	Time, day & date digital displays	Set	1
18	**Printers**		
a	Color Laser printer	Set	1
b	B/W Laser printer	Set	1

SCADA BOQ (DR/BCC Hardware)

Item No.	DRC-Hardware	Estimated	
		Unit	Quantity
1.	SCADA Server	No.	2
2.	FEP server	No.	2
3.	ICCP server	No.	2
4.	ISR Server	No.	2
5.	Historian server	No.	2
6.	NMS server	No.	1
7.	DTS server	No.	1
8.	Web server with load balancing	No.	2
9.	PMS and AV server (Patch Management & Antivirus)	No.	1
10.	**Other Active Devices**		
a.	Development Server (CDS server)	No.	1
b.	QAS server (Quality Assurance server) for patch testing	No.	1
c.	Web/Directory server	No.	1
d.	SMS gateway	No.	1
e.	Developmental console with one TFT	No.	2
f.	DTS/Workstation Console with dual TFTs	No.	2
11	**Storage & Backup Devices**		
A	Network Attached Storage (NAS) or SAN Storage Array with **minimum 20TB usable capacity** (configured in RAID 6 or RAID-TP) to ensure retention of 7 years of historical data and 2 years of online alarms/events for the Ultimate system sizing. The system shall support Active-Active controllers and AI-driven management	No.	1
B	LTO Tape Drive or Disk-based Backup Solution.	No.	1
12	**Switches**		
A	Layer II switch (SCADA LAN)	No.	2
B	Layer II switch (Planning & Development system LAN)	No.	2
C	Layer II switch (FEP) - 24 ports	No.	2
D	Layer II switch (ICCP) - 24 ports	No.	2
13	**Routers**		
A	Router for interfacing IT system & SCADA DR centre	No.	2
14	**Security system (DMZ)**		
A	Firewall including IDS/IPS, Web filtering, VPN	No.	4
B	Layer II switch	No.	4
C	Router cum firewall for ICCP	No.	2
D	Router cum firewall for FEP	No.	2

15	**Other Active Devices**		
A	GPS Time synchronisation system	Set	2
B	Time, day & date digital displays	Set	1
16	**Printers**		
a	Color Laser printer	Set	1
b	B/W Laser printer	Set	1

SCADA BOQ (DCC Software)

Item No.	DCC Software	Estimated	
		Unit	Quantity
1	SCADA including FEP software	Lot	1
2	ISR Software	Lot	1
3	Historian Software	Lot	1
4	DTS software	Lot	1
5	ICCP Software	Lot	1
6	Configuration and Developmental software	Lot	1
7	Network Management Software	Lot	1
8	Software for web server	Lot	1
9	Any other software to meet functional /performance requirement of Section-6 of RFP (Backup software, Antivirus, Virtualization software, Syslog)	Lot	1

SCADA BOQ (DR/BCC Software)

Item No.	DRC Software	Estimated	
		Unit	Quantity
1	SCADA including FEP software	Lot	1
2	ISR Software	Lot	1
3	Historian Software	Lot	1
4	DTS software	Lot	1
5	ICCP Software	Lot	1
6	Configuration and Developmental software(C&DS)	Lot	1
7	Network Management Software	Lot	1
8	Software for web server	Lot	1
9	Any other software to meet functional /performance requirement of Section-6 of RFP (Backup software, Antivirus, Virtualisation software, Syslog)	Lot	1

RTU BOQ

Item No.	SCADA System RTU (S/S)	Estimated	
		Unit	Quantity
	RTU		
1	RTU base equipment comprising panels, racks, sub-racks, Power Supply modules, CPU, interfacing equipment, required converters & all other required items/accessories including complete wiring for all modules for locations mentioned and earthing for each RTU's	Set	215
2	GPRS based Modem for data connectivity from RTU to DCC to integrate with SCADA with (for RTU) including all accessories (canopy, cabling etc)	No.	215

3	GPRS based Modem for data connectivity from DCC to RTU to integrate with SCADA (for DCC/DC and DRC/BCC) (1+1) for 215 Substations including all accessories (canopy, cabling etc)	No.	2
4	SIM for Modem and GPRS Charges (connection in the name of NEA) for 7 years	No.	217
5	Multifunction transducers (MFT)	No.	3225
6	Contact Multiplying Relays (CMRs)	No.	68370
7	Heavy duty relays for Control (HDRs)	No.	8170
8	Dummy Breaker Latching Relays	No.	215
9	Transformer Transducers	No.	430
10	110 V DC to 48 V DC converter with all accessories, cable etc. for RTU & Modem backup power	No.	215
	LDMS solutions		
10	LDMS system	No.	215
10 (a)	Furniture for LDMS system (one table and one chair each Substation suitable for operation)	Set	215
10 (b)	Power Backup for LDMS	Set	215
10 (c)	Workstation with 17" (inch) TFT & CPU with windows licenses and antivirus with 5 years subscription	Set	215
	Firewall		
11	Firewall (for substations where OTN is not provided)	No.	70
	Converter/Gateway		
12	IEC-61850 to IEC-60870-5-104 Protocol Converter / Gateway – Industrial grade, redundant power supply, supports MMS/GOOSE mapping, time synchronization (NTP/GPS), secure IEC-104 link to DCC	No.	18
	Switch		
13	Industrial Grade Optical Fiber Switch (8 port for 5/10/20 kms having Ethernet, VLAN, Supporting, Remote reset, Manageable L2 Switch) with all accessories - at substations with fibre connectivity	Nos	145
	Test Equipments for RTU		
14	RTU Database Configuration & Maintenance Software tool	No.	10
15	Master Station cum RTU Simulator & Protocol analyser software tool	No.	10
16	Laptop PC for above software tools along with interfacing hardware including Industrial Layer-2 Switch.	No.	10

------End of Chapter 15-----

APPENDIX: SCADA

LIST OF ABBREVIATIONS

- ADSS: All-Dielectric Self-Supporting
- ANSI: American National Standards Institute
- AMC: Annual Maintenance Contract
- AOR: Area of Responsibility
- BCC: Backup Control Center
- BOQ: Bill of quantity
- CB: Circuit Breaker
- CMR: Contact Multiplying Relay
- CIM: Common Information Model
- CMOT: Common Management Information Protocol
- COSEM: Companion Specification for Energy Metering
- CPU: Central Processing Unit
- DCC: Distribution command center/SCADA Control center
- DAT: Digital Audio Tap
- DC: Data Concentrator
- DCDB- Direct Current Distribution Board
- DDoS: Distributed Denial of Service
- DLMS: Device Language message specification
- DMZ: Demilitarized zone
- DNS:- Domain Name System
- DR: Data Recovery
- DRC: Disaster Recovery Center
- DRR: Disaster Replica Recovery
- DTS: Dispatcher training simulator
- FAT: Factory Acceptance Test
- FMS: Facility Management Services
- FTP: File Transfer Protocol
- ESB: Enterprise service bus

- ECMA: European Computer Manufacturers Association
- FCC: Federal Communications Commission
- GOOSE: Generic Object-Oriented Substation Even
- GPS: Global positioning system
- GPRS: General Packet Radio Service
- GUI : Graphical User Interface
- HDR: Heavy Duty Relays
- HDD: Hard Disk Drive
- HI : Historian Information
- HIPS: Host-based IPS
- HTTP : Hyper Text Transfer Protocol
- ICCCM: Inter-Client Communications Conventions Manual
- ICCP: Inter Control Center Protocol
- ICS: Industrial Control System
- IPS: Intrusion prevention system
- ISP: Internet Service Provider
- IEC: International Electro technical commission
- ISO: International organizations for standardizations
- IEC: International Electrotechnical Commission
- IEEE: - Institute of Electrical and Electronics Engineer
- ISR: Information storage & retrievals
- IRIG: Inter-Range Instrumentation Group
- IT : Information Technology
- LAN: Local Area Network
- LDAP: Lightweight Directory Access Protocol
- LDMS Local Data Monitoring System
- LSA: Load Shed Application
- LDC Load Dispatch Center
- MFT: Multifunction Transducers
- MMS: Manufacturing Message Specification
- MITM: Man-in-the-Middle
- MPLS : Multiprotocol Label Switching
- MTS : Model Technical specification

- MTBF: Mean Time Between Failures
- MB: Mega Byte
- MCD: Momentary change Detection
- NMS: Network Management system
- NOC: Network Operation Center
- ODAR: Outage data analytics and reporting
- ODBC: Open Data Base Connectivity
- OEM: Original Equipment Manufacturer
- OFC: Optical Fiber Cable
- OPC: OLE for Process Control
- OLE:- Object Linking and Embedding
- OS: Operating System
- OLTC: On-Load Tap Changer
- OTA: Over the Air
- OT Operational Technology
- O&M: Operation & Maintenance
- PLC: Programmable Logic Capabilities
- RAM: Random Access Memory
- RDBMS: Relational database management system
- RTU: Remote Terminal Unit
- RTDB Real Time Database
- RF: Radio Frequency
- SAN: Storage area network
- SAT: Site Acceptance Test
- SCADA: Supervisory Control and Data Acquisition
- SCBO: Select Check Before Operation
- SLA: Service Level agreement
- SI: System Integrator
- SNTP: Simple Network Time Protocol
- SNMP: Simple Network Management Protocol
- SMTP: Simple Mail Transfer Protocol
- UDP: (User Datagram Protocol)
- SOA: Service-Oriented Architecture

- SOC: Security operation center
- SOE: Sequence of Events
- SOP: Safe Operating Procedures
- SQL: Structured Query Language
- S/S: Substations
- SSO: Single Sign On
- SSL: Secure Socket Layer
- TCP/IP: Transmission Control Protocol/Internet Protocol
- TFT : Thin-Film Transistor
- TB: Tera Byte
- UPS: Uninterrupted Power Supply
- URL: Uniform Resource Locator
- UDP: User Datagram Protocol
- VPS: Video Projection System
- VDU: Visual Display Unit
- VPN: Virtual Private Network
- XML: Extended Markup Language

NEPAL ELECTRICITY AUTHORITY

(An Undertaking of Government of Nepal)
Project Management Directorate
Distribution Line and Substation Department

NEA DIGITAL NETWORK AND SCADA EXPANSION PROJECT

BIDDING DOCUMENT
FOR
Procurement of Plant for
Design, Supply, Installation and Commissioning
of
NEA Digital Network and SCADA Expansion

(Procurement of Plant)

Single-Stage, Two-Envelope
Bidding Procedure

Issued on:	**22nd February 2026**
Invitation for Bids No.:	**PMD/ETDSP/NDNSEP-082/83-01**
OCB No.:	**PMD/ETDSP/NDNSEP-082/83-01**
Employer:	**Nepal Electricity Authority**
Country:	**Nepal**

VOLUME –II (Part-C)

NEA Digital Network & SCADA Expansion Project
Distribution Line and Substation Department
Project Management Directorate
Matatirtha, Kathmandu, Nepal
Telephone: 01 5164099

(Volume -II, Part-C)
Technical Specifications-
ADSS

1. Specification of for Metal Free ADSS Fiber Optic Cable and associated hardware & fittings

This Specification covers the functional & technical specifications of ADSS (All Di-Electric Self Supporting) Fiber Optic cabling and associated hardware & fittings.

1.1 Description

This Specification covers the functional & technical specifications of ADSS (All Di-Electric Self Supporting) Fiber Optic ADSS Optical Fiber Cable shall be installed on 33kV/11kV lines and may also be installed on LT lines. The estimated cable route length requirements are indicated in the price schedules. However, the Contractor shall supply & install the ADSS Optical Fiber Cable as required based on detailed site survey to be carried out by the Contractor during the project execution.

1.2 Functional Requirement

The design and construction of ADSS metal free optical Fiber cable shall be inherently robust and rigid under all conditions of installation, operation, adjustment, replacement, storage and transport. The cable shall possess good performance characteristics such as anti-impact, anti- vibration, anti-bending, prevention of thermal aging etc. All the elements consisting of ADSS cable shall be non-metallic.

The design and construction of ADSS metal free optical Fiber cable shall be inherently robust and rigid under all conditions of installation, operation, adjustment, replacement, storage and transport. The cable shall be able to work in the environment prevailing in Nepal, including high altitude and saline/corrosive atmospheres, and must be protected against corrosion.

The cable shall be suitable for installation on electric lines. The Maximum Electric Field Strength (MEFS) at the proposed attachment points shall be defined by the Contractor during the site survey, The offered cable design and materials (e.g., Aramid yarn/sheath) shall be rated for the determined MEFS and must prevent tracking and corona discharge

Life of cable shall be at least 25 years. Necessary statistical calculations shall be submitted by the manufacturer, based upon life of the Fiber and other component parts of the cable. The cable shall meet the cable aging test requirement.

It shall be possible to install the ADSS optical Fiber cable with Accessories and Fixtures as per IEC 61284, IEEE 1222 International Standard. If any special Accessories and Fixtures are required for installation of the ADSS optical Fiber cable, the same shall be provided along with the cable. The

accessories required for mounting the splice closure on towers shall also be supplied along with splice enclosure.

The ADSS optical Fiber Cable shall be suitable and compatible with the dimensions, fixing, terminating and splicing arrangement of the splice closure supplied along with the cable & vice versa. The manufacture shall indicate the type, make and the model no. of the splice closure to be supplied along with cable. The cable supplied shall also meet other requirement of the splice enclosure Universal type compliant with IEC 61753-1 (Category G), Telcordia GR-771-CORE or equivalent International Standard.

The Self-Supporting Metal Free ADSS Optical Fiber cable shall be designed and manufactured supplied under this contract as per IEC 60794-4-20 / IEEE 1222 international standard or with latest amendment, if any, to meet the following conditions of operation, installation and storage:

For the specific span and environmental conditions listed below

a) Maximum Length: 100 meters
b) Maximum Ice loading: 0 Kg per meter
c) Operational Wind velocity: 100 kms. per hour
d) Sag of the span length:
   i. Maximum Sag allowed without excess load: 1% of the span length
   ii. Maximum Sag allowed with excess load: 2% of the span length
e) Operating Temperature: -40 ℃ to 70 ℃
f) Installation Sag and Tension calculations as per IEEE 1222. g)
g) Minimum bending radius: 10D (D – Diameter of cable)
h) Minimum distance of cable from Phase Conductor on 33/11 kV line: 1.5 Meter.

1.3 Technical Requirement

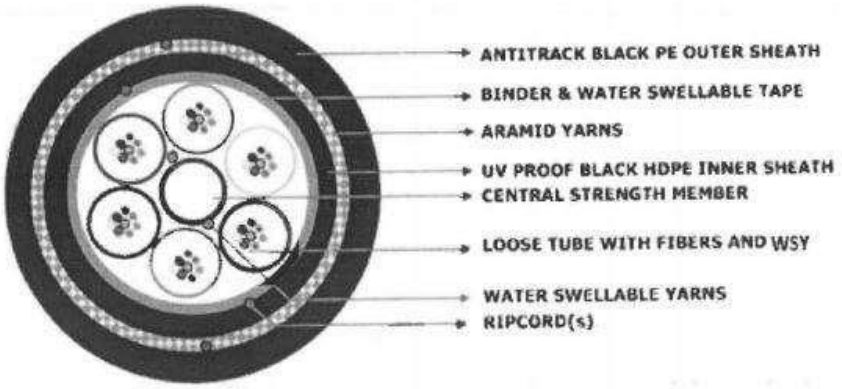
DWSM (Dual Window Single Mode) Optical Fiber used in manufacturing optical fiber cables shall be as per ITU-T Rec G.652D. The specifications of fiber shall be as per Table given below.

Table 4: DWSM Optical Fiber Characteristics

Fiber Description:	Dual-Window Single-Mode
Mode Field Diameter:	8.6 to 9.5 μm (± 0.6μm)
Cladding Diameter:	125.0 μm ± 1 μm
Mode field concentricity error	≤ 0.6μm

Cladding non-circularity	≤ 1%
Cable Cut-off Wavelength lcc	≤ 1260 nm
550 nm loss performance	As per ITU-T G.652 D
Proof Test Level	≥ 0.69 Gpa
Attenuation Coefficient:	@ 1310 nm ≤ 0.34 dB/km @ 1550 nm ≤ 0.19 dB/km (typical), 0.21 dB/km (maximum)
Chromatic Dispersion; Maximum: Zero Dispersion Wavelength: Zero Dispersion Slope:	18 ps / (nm x km) @ 1550 nm 3.5 ps / (nm x km) 1288-1339nm 5.3 ps / (nm x km) 1271-1360nm 1300 to 1324nm 0.092 ps / (nm^2xkm) maximum
Polarization mode dispersion coefficient	≤ 0.2 ps/km^½
Temperature Dependence:	Induced attenuation ≤ 0.05 dB (-60°C - +85°C)
Bend Performance:	@ 1310 nm (75±2 mm dia Mandrel), 100 turns; Attenuation Rise ≤ 0.05 dB @ 1550 nm (30±1 mm radius Mandrel), 100 turns; Attenuation Rise ≤ 0.05 dB @ 1550 nm (32±0.5 mm dia Mandrel, 1 turn; Attenuation Rise ≤ 0.50 dB

1.4 ADSS Optical Fiber Cable Construction Specifications for Totally Dry (Gel-Free) Core Design



Typical Structural Drawing for 48 Fiber of Cable

Secondary Protection:

The primary coated Fibers may be protected by loose packaging within a tube or tubes which shall

contain water swellable yarn to prevent water ingress in loose tube.

Number of Fibers: 48

Strength Member: Solid FRP non - metallic strength member in the centre of the cable core shall be provided. The strength member in the cable shall be for strength and flexibility of the cable and shall have anti buckling properties. This shall also keep the Fiber strain within permissible values.

Cable Core Assembly:

Primary coated Fibers in loose tubes, stranded together around a central strength member (using helical or reverse lay techniques), shall form the cable core.

Core Wrapping:

The main cable core containing Fibers shall be wrapped by layer/layers of water swellable tape & binder (as per IEC 60794 series)

Moisture barrier (protection): The main cable core (containing Tube/FRP & Core wrapping) shall be protected by water swellable yarn as per IEC 60794 water penetration requirements

Inner Sheath:

A non-metallic moisture barrier sheath may be applied over and above the cable core. The core shall be covered with tough weather resistant High-Density Polyethylene (HDPE) sheath, black in colour. Thickness of the sheath shall be uniform and shall not be less than 1.0mm. The sheath shall be circular, smooth, free from pin holes, joints, mended pieces and other defects. Reference test method to measure thickness shall be as per IEC 189 para 2.2.1 and Para 2.2.2.

Note: HDPE material (in black colour) from the finished cable, shall be subjected to following tests (on sample basis) and shall conform to the requirement of the material as per s per IEC 60794-1-2 and ASTM D1248.

i. Density
ii. Melt flow index
iii. Oxidative Induction time
iv. Carbon black content
v. Carbon black dispersion
vi. ESCR
vii. Moisture content
viii. Tensile strength and elongation at break

Reinforcement:

The ADSS optical Fiber cable shall be helically reinforced with Aramid Yarn in the periphery over the inner sheath. The Aramid Yarn shall be uniformly and equally distributed on the entire periphery (circumference) of the cable. The quantity of Aramid Yarn shall be sufficient to ensure the cable meets the Maximum Working Tension (MWT) and sag limits (1% initial, 2% final) for the specified span lengths and wind/ice loading conditions defined in the Functional Requirements. The design shall ensure zero fiber strain at MWT. The Aramid Yarn shall comply with IEC 60794-4-20.

Outer Jacket:

A circular and uniform tough weather resistant polyethylene compound Antitrack Polyethylene material sheath/Jacket, black in colour, (UV Stabilised) shall be provided over and above the reinforcement of Aramid Yarn. The thickness of the outer sheath/Jacket shall not be less than 1.8mm. The sheath shall be free from pin holes, joints, scratches, mended pieces and other defects etc. and it shall have smooth finish.

Note: Antitrack PE material (in black colour) from the finished cable, shall be subjected to following tests (on sample basis) and shall conform to the requirement of the material as per IEC 60794-1-2 and ASTM standards.

i. Density
ii. Melt flow index
iii. Oxidative Induction time
iv. Carbon black content
v. Carbon black dispersion
vi. ESCR
vii. Moisture content
viii. Tensile strength and elongation at break

Cable diameter:

The manufacturer shall define the cable diameter. The finished cable diameter shall be determined by the Manufacturer to meet the specified mechanical and electrical performance. The manufacturer shall guarantee the diameter in the technical data sheet.

RIP Cord:

a) The suitable water blocking ripcords (two each for Inner & Outer sheath) shall be provided which shall be used to open the inner and outer sheath of the cable. It shall be capable of consistently slitting the sheath without breaking for a length of 1 meter at the installation temperature. The rip cord(s) shall be properly waxed to avoid wicking action and shall not work as a water carrier.

b) The ripcord used in the cable shall be readily distinguishable from any other components (e.g. Aramid Yarn etc.) utilized in the cable construction.

Details of Technical parameters shall be shall be guaranteed by the bidder based on design calculations.

DRY CORE CABLE DESIGN

The following parameters of the component parts of the cable are to be taken in to account while designing and manufacturing the optical Fiber cables of the required Fiber count. These parameters shall be checked during evaluation of the OF cables: A

S.N.	Parameter	Unit	48 Fiber OF Cable
1	FRP Rod EAA Coated	mm	2.5+0.1/-0.0
2	FRP up jacketing thickness	mm	0
3	Tube ID (min)	mm	1.7
4	Tube OD	mm	2.4 ± 0.1
5	No of Fiber / tube	No	12
6	Color of Fiber		BL, OR, GR, BR, SL, WH, RD, BK, YL, VI, PK, NAT
7	No of loose tubes	No	4
8	Color of loose tubes		BL, OR, GR, BR
9	No of dummy cord	No	2
10	Tube stranding lay over length	mm	90-110
11	Aramid Yarns-Min	Kg/Km	10
12	Cable diameter	mm	14.5 ± 0.5
13	Nominal cable weight	Kg/Km	140-170
14	Cable to be designed to Fiber strain value of.	%	0.1
15	Excess Fiber length	%	0.7
16	Cable to be tested at defined load for fiber strain value of	%	0.25

1.5 Raw Material

The cable shall use high-quality raw materials from ISO 9001 certified manufacturers, compliant with **ASTM** or **IEC** material specifications. The change in the design of the optical cable shall call for fresh type testing. The material used in optical Fiber cable must not evolve hydrogen that will affect the Fiber loss.

A test certificate from a recognized laboratory or institute may be acceptable.

1.6 Cable Material Compatibility

Optical Fiber, buffers/core tubes, and other core components shall meet the requirements of the compatibility with buffer/core tube filling material(s) and/or water-blocking materials that are in direct contact with identified components within the cable structure as per IEC 60794-1-2.

1.7 Safety Requirement

The material used in the manufacturing of the optical Fiber cables and for use in splicing and maintenance shall be non-toxic and dermatologically safe in its lifetime and shall not be hazardous to health.

1.8 Operating requirement

The design and construction of ADSS metal free optical Fiber cable shall be inherently robust and rigid under all conditions of operation, adjustment, replacement, storage and transport. The optical Fiber cable shall be able to work in the environment prevailing in Nepal. The Contractor shall take into consideration the UTS of transmission line while designing the ADSS Cable.

The ADSS optical Fiber cable shall work satisfactorily in electrical field environment of 33 kV and shall not degrade with presence of electrical field. The cable shall be installed on 33 kV lines and the fittings location shall be so selected the field at the point of installation shall not exceed 33 kV.

The bidder may consider the design span length of 100 meter for bidding purpose. However, actual span length shall be determined by the Contractor during the site survey.

The supplied cable shall meet the span, wind loading requirement of the specified location where the cable is to be installed.

1.9 Optic Fiber Cable Lengths

The fiber optic route lengths are as specified in appendices and price schedules. The lengths specified in appendices are route lengths; however, the actual fiber cable length shall exceed the route lengths on account of extra cable requirement due to loop, jointing & splicing.

The exact cable lengths shall be determined by the Contractor during the survey. The same shall be

used by the Contractor for final link design during the detailed engineering of the project. The payment will be made for installation on the executed route length only. Up to 3% wastages of OFC shall be allowed for specified service loops, lengths for wastage, installation/working for FO cable, sag, joints, terminations etc. during material reconciliation after measurement.

1.10 Cable Ends

Both cable ends (the beginning end and end of the cable reel) shall be sealed and readily accessible. Minimum 5 meter of the cable of the beginning end of the reel shall accessible for testing. Both ends of the cable shall be kept inside the drums and shall be located so as to be easily accessible for the test. The drum (confirming to latest IEC Specs) should be marked to identify the direction of rotation of the drum. Both ends of cable shall be provided with cable pulling (grip) stocking and the anti-twist device (free head hook).

Anti-twist device (Free head hook) shall be provided attached to both ends of the cable pulling arrangement. The arrangement of the pulling eye and its coupling system along with the anti- twist system shall withstand the prescribed tensile load applicable to the cable.

1.11 The nominal drum length

Generally, the length of ADSS optical Fiber cable in each drum shall be 2 km ± 5 %. However, it can be optimized as per site conditions during detail engineering. The drum shall be marked with arrows to indicate the direction of rotation. Packing list supplied with each drum shall have at least the following information: Drum no., Type of cables, Physical Cable length, No. of Fibers, Length of each Fiber as measured by OTDR, The cable factor – ratio of Fiber/cable length, Attenuation per km. of each Fiber at 1310 & 1550 nm, User's/consignee's name, Manufacturer's Name, Month, Year and Batch no., Name of the route.

1.12 Optical Fiber Strain

The following shall be ensured while performing sag tension calculations:

(a) The cable strain margin is defined as the maximum cable strain at which there is no Fiber strain.

(b) The no Fiber strain condition is defined as Fiber strain of less than or equal to 0.05%, as determined by direct measurement through IEC/ETSI(FOTP) specified optical reflectometry techniques. There should not be any Fiber strain at any condition

The Contractor shall offer suitable ADSS optical Fiber cable for various spans for the ADSS FO cable meeting the following conditions for Employer's approval: The ground clearance & Electrical clearance shall be met for the actual site conditions.

1.13 Cable Marking

The cable marking shall be imprinted and indelible (indented). The marking on the cable shall be indelible of durable quality and at regular intervals of one meter length. The alternatively permanent printing with the laser shall also be acceptable. In case of laser printing method; the impression shall not exceed the depth of 0.15 mm. The accuracy of the sequential marking must be within –0.25% to +0.5% of the actual measured length. The markings on the cable must not rub off during normal installation.

The marking shall be of clearly contrast colour on the black HDPE sheath in case hot foil indentation or laser printing method is used. The colour used must withstand the environmental influences experienced in the field.

Two orange colour (UV stabilized) lines of minimum 3 mm width diametrically opposite to each other, continuous over the length of the cable shall be applied (marked) for easy identification of this cable from other cables.

The type of legend marking on O.F. cable shall be as follows:

(i) Company Legend
(ii) Legend containing international acceptable Laser symbol
(iii) Type of cable i.e., Slotted or Loose Tube or Uni-tube (Central Tube)
(iv) Type of Fiber ie. DWSM
(v) Number of Fibers
(vi) Year of manufacturer
(vii) Sequential length marking
(viii) Employer's Name

1.14 Installation, Accessories and Fixtures for ADSS Cable

The scope of supply of the Metal Free ADSS Optical Fiber Cable includes the assessment, supply and installation of all required installation accessories and fixtures. The Bidder shall provide documentation justifying the adequacy and suitability of the hardware used. To ensure their satisfactory performance, the Contractor shall determine the exact requirements of all accessories and fixtures used to install and secure the cable.

The cable hardware accessories and fixtures shall follow the general requirements regarding design, materials, dimensions & tolerances and markings etc. as specified in EC 61284, IEEE 1222 International Standard with latest amendment. The cable accessories & fixtures drawing & Data

Requirement Sheets (DRS) document shall consist of three parts: (1) A technical particulars sheet (2) An assembly drawing i.e., level 1 drawing and (3) Component level drawings i.e., level 2 & lower drawings. All component reference numbers, dimensions and tolerances, bolt tightening torques & shear strength and ratings such as UTS, slip strength etc. shall be marked on the drawings.

The required joint box shall also be provided by the Contractor and the details of which shall be submitted for Employer's approval. The joint box shall comply to ingress protection class IP 66 or better. The in-line splice enclosures shall be metallic type and support mechanical opening and closing.

The required strengthening of existing structures/towers/poles shall be carried out by the Contractor for installation of offered ADSS cable.

As the ADSS cable is designed for 100 m span for self-supporting condition, for the span greater than 50 m, the additional strength wire along with the clipping arrangement to support the ADSS cable for installation of ADSS cable system shall also be provided by the Contractor at no additional cost to the Employer. However, the actual span lengths may vary at site and the fittings & accessories shall be provided as per site requirement.

The above requirement of, strength wires, strengthening of existing structure/poles/towers shall be submitted by the Contractor for Employer's approval and same shall be provided as per approval.

The typical details of Installation fixtures are given below, however contractor to supply any additional items required for successful installation of Self-Supporting Metal Free ADSS Optical Fiber Cable without any extra cost to employer:

S.N.	Item Details	Unit	Required Quantity/Pole
A	**Tension Fitting set**		
1	D Shackle or J Tension Hook	Set	2
2	Turn Buckle	Set	2
3	Extension Link	Set	2
4	Clevis Thimble	Set	2
5	Protective Helix (T)	Set	2
6	Terminating Helix	No.	2
7	Jumper Cable Clamp	Set	1
8	Pole clamp – tubular	Set	1
B	**Suspension Fitting set**		

1	Twisted Eye Link	Set	1
2	Protective Helix (S)	Set	1
3	Armor Grip Helix	Set	1
4	Suspension Clipper with Elastomer Pad	Set	1
5	Spiral Vibration Damper (SVD)	Set	2
6	Pole clamp – (as per pole design tubular, rail etc.)	Set	1
C	**Pole Mounted Stay Clamp (light) for Jumper clamp**	No.	1
D	**Demountable Pulley with rubberized wheel**	Set	1
E	**Adjustable cable storage bracket**	Set	1

1.15 Optical Fiber Splicing

Splicing of the optical Fiber cabling shall be minimized through careful planning. Mid-span splices are generally not permitted. However, in unavoidable site conditions, they may be allowed subject to Employer's prior approval. All required splices shall be planned to occur within facilities or on tower structures. All optical Fiber splicing shall comply with the following:

(a) All Fiber splices shall be accomplished through fusion splicing.

(b) Each Fiber splice shall be fitted with a splice protection sheath fitted over the final splice.

(c) All splices and bare Fiber shall be neatly installed in covered splice trays. No more than 12 (twelve) Fibers shall be installed in each splice tray.

(d) For each link, bi-directional attenuation of single mode fusion splices measured at 1550 nm shall not average more than 0.05 dB. The bi-directional splice loss of each splice shall not exceed 0.1 dB when measured at 1550 nm.

(e) For in-line splicing, Fiber optic cable service loops of adequate length shall be provided so that all splices occurring at tower structures can be performed at ground level.

1.16 Optical Fiber Termination and Splicing

Optical Fiber terminations shall be done in Fiber Optic Distribution Panels (FODP) at Substations and FMS (Fiber Management System) at RMU (Ring Main Unit) locations. The Contractor shall provide rack /wall mounted Fiber Optic Distribution Panels (FODPs) & FMS that shall be 1U, 2U, 3U like size and able to fit in cabinet at GO switch panel and Sub-Station FODP. The location of FODP rack shall be fixed by the Contractor, with the Employer's approval.

The technical specification of FODP is given in 2.3 (below) of this specification.

1.17 Optical Fiber Connectors

Optical Fibers shall be connectorized with FC-PC type connectors preferably. Alternatively, connector with matching patch cord shall also be acceptable. Fiber optic couplings supplied with FODPs shall be appropriate for the Fiber connectors to be supported. There shall be no adapters.

1.18 Service Loops

For purposes of this specification, cable and Fiber service loops are defined as slack (extra) cable and Fiber provided for facilitating the installation, maintenance and repair of the optical Fiber cable plant.

(a) Outdoor Cable Service Loops: In-line splice enclosures installed outdoors and mounted on the utility towers, shall be installed with sufficient Fiber optic cable service loops such that the recommended minimum bend radius is maintained while allowing for installation or maintenance of the cable to be performed in a controlled environment at ground level.

(b) Indoor Cable Service Loops: FODPs shall provide at least three (3) metres of cable service loop. Service loops shall be neatly secured and stored, coiled such that the minimum recommended bend radius are maintained.

(c) Fiber Units Service Loops: For all Fiber optic cable splicing, the cable shall be stripped back a sufficient length such that the fan-out of Fiber units shall provide for at least one
(1) meter of Fiber unit service loop between the stripped cable and the bare Fiber fan- out.

(d) Pigtail Service Loops: Connectorized pigtails spliced to bare Fibers shall provide at least 1 meter of service loop installed in the FODP Fiber organizer and at least one (1) meter of service loop to the couplings neatly stored behind the FODP coupling panels.

(e) Fiber Service Loops: At least 0.5 meter of bare Fiber service loop shall be provided on each side of all Fiber splices. The bare Fiber service loops shall be neatly and safely installed inside covered splice trays.

1.19 Anti-Rodent Compliance

ADSS cable is to be installed on rodent prone areas; ADSS should have anti rodent complied

1.20 Methodology for Installation and Termination

a. Installation Techniques

The techniques used in installation of ADSS Optical Fiber Cables are described here. With the proper installation hardware and skilled resource, any of these methods can be used to install ADSS cable. Many a times, it will become necessary to use a combination of these methods to achieve full installation. Selection of the specific technique (i.e., Moving Drum method, Stationary Drum method or Manual Installation method), or a combination thereof, shall largely depend on the actual site conditions. The contractor shall select the most appropriate installation technique suitable to the site conditions.

b. Moving Drum method

In this method the cable is pulled directly from the cable drum mounted on a moving vehicle as it drives along the pole line. The cable drum must be mounted on a proper support to allow easy cable pay off. At the dead-end point, the cable is terminated using Termination Assembly sets and tensioned using turnbuckles to maintain cable sag within permissible value. To start installation, park the vehicle with the cable drum approximately 15 - 20 meters away from the pole facing away from it down the pole line. The cable must pay off from top of the drum towards the rear of the vehicle Install the termination supports and temporary hooks on the poles at the starting point and subsequent poles. Pull off the necessary amount of slack, lift the dead-end to the top of the pole and mount on the termination assembly. Once the cable is fixed at both ends with at the terminating assemblies, carry out tensioning. After the cable section is properly tensioned and secured at both ends lift the cable out of the hooks at each of the intermediate pole and support it with the suspension set assemblies.

c. Stationary Drum Method

In this method of ADSS cable installation, the cable is pulled along the cable route through temporary support hardware. Stationery drum installation method requires installation of temporary support hardware such as pulley blocks.

A rope wound on the tension limiting winch is passed through the pulleys and connected to the cable on the drum installed on a stand which allows free rotation of the drum. The pulling load should normally not exceed 60% of the maximum permissible cable tension recommended by cable supplier.

The cable drum and winch locations must have vehicular access. The cable drum should always be placed on levelled ground so that its flanges are vertical thus avoiding rubbing of cable against flanges. The orientation should be such that the cable pay-off is directly in the direction of pull. Always pay-out the cable from top of the drum and not from bottom. The drum should

have provision to allow controlled pay-out of cable. Cable pay-out needs to be controlled to prevent free running or jerking.

Once the cable is completely pulled end to end, it is then ready for installation of permanent supporting system of terminating and suspension set assemblies at required locations and tensioning for sag control.

d. Manual Installation method

Manual installation method technique is similar to stationary drum method, except that in this case the cable is uncoiled from the drum and placed on the ground in the shape of 8. The pulling operation is same as in stationary drum method. The hardware requirement and pulling equipment also remains same.

For pulling in both directions, two loops of shape of 8 can be made and each can be pulled in separate directions. Loops of size 4 to 5m x 1.5m should be sufficient in most cases.

e. Installation of Accessories

1. Pole Clamp

Prior to fixing any temporary supports / stringing blocks or permanent cable suspension/termination assemblies, it is necessary to fix pole clamps. Appropriate type of pole clamps will be required depending on the shape of the pole. The two halves shall be opened and fixed at the specified height using tightening bolts.

2. Terminating (or dead End) Assembly

Termination assemblies are required at dead ends locations where:

i. Cable needs to be terminated at the end facility
ii. Loops are to be kept for future maintenance activities

For double sided termination assembly 2 sets would be required. To fix a termination Assembly following accessories are required:

i. Protective Helix on the cable,
ii. Terminating Helix with a thimble,
iii. Clevis Thimble,
iv. Spiral Vibration Damper

3. Suspension Assembly

ADSS optical Fiber cable shall be supported on all intermediate poles between two

terminating poles using the pole clamp and a suspension assembly set.

To fix a suspension Assembly following accessories are required:

i. Protective Helix on the cable,
ii. Suspension Helix,
iii. Clevis Thimble,
iv. Spiral Vibration Dampers

4. Installation Cable Loop / storage / Joint Closure

Cable loops are to be provided for future maintenance purposes at regular spacing. A fixture is required to be installed. Excess cable is then wound & kept on support. The fixture provides a means to ensure Proper bend radius is maintained. Separate clamp is required for installation of Joint Closures.

5. Supporting Jumper Cable Clamp

Jumper cable hanging between a pair of Termination Assemblies installed at locations where there is sharp change in direction need to be supported with a special twisted link. To support jumper cable, use already installed clamp.

6. Cable Tensioning

After the required Length of cable has been placed, the cable shall be properly tensioned before it is permanently secured into suspension assemblies. The temporary dead end should be installed 4 to 5 m from the pole so that after complete tension is applied, appropriate permanent termination assembly set can be installed while the cable is in tension. The chain hoist will also need to be tied to the pole directly using a sling and on to pole clamp.

Once the cable sanction are under the required tension and the sag is within limits (i.e. less than 1% of span), the “free” end of the cable used for tensioning is fitted with termination assembly set and terminated. Once the load is transferred on to permanent termination end, the temporary arrangement shall be removed.

7. Machinery / Equipment / Tools

Ropes and Light weight ladder for installation of termination / suspension assemblies, clamps etc. Temporary supports, dynamometer, chain hoists, temporary dead ends steel cables, etc. required during cable laying and / or cable pulling and cable preparation kits,

etc. as applicable will have to be arranged by the Agency.

Van with portable splicing machines and OTDR, power meter, cable preparation kits, etc. for splicing and testing of installed ADSS Optical Fiber Cable.

Other tools and tackles shall include wrenches, spanners, screwdrivers, hummer, ropes etc.

All safety equipment such as safety belts, insulating and cotton gloves and hard hats, fluorescent vests etc. as required.

8. Other guideline for ADSS Cable installation

All optical Fiber cable termination, installation, stringing and handling plans, guides and procedures, and engineering analysis shall be submitted to the Employer for review and approval in the engineering/design phase of the project, prior to establishing the final cable lengths for manufacture. Installation procedures including details of personnel and time required shall be documented in detail and submitted to Employer for approval. All installation practices shall be field proven and ISO accredited.

All cable segments shall include service loops as specified in this specification. The maximum allowable stringing tension, maximum allowable torsional shear stress, crush strength and other physical parameters of the cable shall not be exceeded. The preventative measures to be taken shall be documented in detail and submitted to Employer in advance of installation.

Optical Fiber attenuation shall be measured after installation and before splicing. Any increase in attenuation or step discontinuity in attenuation shall not be acceptable and shall constitute a cable segment failure. In the event of cable damage or any Fiber damage, the complete section (tension location to tension location) shall be replaced as mid-span joints are not acceptable.

Any or all additional steel work or modifications required to attach the Fiber cabling to the overhead transmission/ distribution line towers shall also be carried out by the Contractor. It shall be the Contractors responsibility to provide adequate communications among all crew members and support staff to ensure safe and successful installations.

1.21 Cable Raceways

To the extent possible, existing cable raceways shall be utilised. The Contractor is required to provide and install any additional indoor cable raceways which may be required for proper implementation of the Fiber optic cabling system. This requirement shall be finalised during survey.

The cable raceways shall conform to the following:

(a) All cable raceways shall be sized to support full loading requirements plus at least a 200% safety loading factor.

(b) Indoor cable raceways shall be fabricated from construction grade aluminium, galvanized iron or anodized sheet metal or any other suitable material approved by the Employer. Suitable anti-corrosion measures shall be provided. Steel fabricated raceways shall be finished inside and out, treated to resist rust and to form a metal-to- paint bond.

(c) Mechanical construction drawings of the cable raceways shall be submitted for Employer's information & review.

1.22 Testing

a. Type Testing

The Contractor shall submit along with their bid the earlier carried out type test reports for the offered ADSS optical Fiber cable, its accessories and fixtures etc. meeting the requirement. The Contractor shall submit the type test reports for a cable of similar or higher fiber count and similar construction/voltage rating for the tests. All items should have been type tested as per relevant standards for the tests and the Contractor shall submit the test reports and certificates along with the bid.

Type Testing on ADSS Optical Fiber Cable

The type test on the ADSS Cable shall be as per procedure mentioned in IEC 60794-1-2 series. The Fiber should have been type tested as per relevant international standards for the tests listed in Table given below.

S.N.	Name of Test
1	Tensile strength Test
2	Abrasion Test
3	Crush Test (Compressive Test)
4	Impact Test
5	Repeated Bending
6	Torsion Test
7	Kink Test
8	Cable Bend Test

9	Snatch Test
10	Cable Bend Test at High & Low Temperature
11	Temperature Cycling
12	Cable Aging Test
13	Cable Freezing Test

S.N.	Name of Test
14	Water Penetration Test
15	Test of Figure of Eight on the cable
16	Flexural Rigidity Test on the optical Fiber cable
17	Static Bend Test
18	Cable Jacket Yield Strength and Ultimate Elongation
19	Drip Test
20	ECSR Test
21	UV Resistance Test
22	Embrittlement Test of Loose Tube
23	Kink Resistance Test on the Loose Tube
24	Drainage Test for Loose Tube
25	Check of Easy removal of Sheath
26	Check of the effect of Aggressive Media on the Cable
27	Electrical Test
28	Aeolian Vibration Test (Type Test)
29	Galloping Test
30	Sheave Test
31	Creep Test
32	Tracking & Erosion Test

Type Testing for ADSS FO Cable Accessories & Fixtures

The type test on the ADSS Cable shall be as per procedure mentioned in IEC 61284 and BS EN 50483 series, if any. The applicability of the tests for the particular type of accessories and fixtures shall be as given below.

S.N.	Name of Test
1	Verification of dimensions: Applicable to all fittings
2	Tensile strength test: Applicable to tension & suspension clamp assemblies
3	Tensile strength test for helically formed product
4	Slip Strength Test
5	Resilience Test
6	Galloping / Fatigue test
7	Aeolian Vibration Test
8	Tension and Attenuation Test (Dead End Assembly)
9	Wrapping Test
10	Galvanising Test
11	Hardness Test of Elastomer pad

b. Factory Acceptance Testing

Factory Acceptance Tests on ADSS optical Fiber cable

The tests listed in Table given below shall be carried out as Factory Acceptance Test for ADSS optical Fiber cable meeting the requirements specified in this Chapter.

S.N.	Factory Acceptance Test
1	Attenuation Coefficient (1310, 1550): By EIA/TIA 455- 78A or OTDR
2	Point discontinuities of attenuation: By EIA/TIA 455- 78A or OTDR
3	Visual Material verification and dimensional checks as per approved drawings
4	Water Ingress test
5	Tensile strength test / Strain test
6	Impact test
7	Kink test
8	Environmental test
9	Crush Test
10	Drip test

Factory Acceptance Tests on ADSS cable accessories & fixtures

The FAT on accessories & fixtures of ADSS optical Fiber cable shall be carried out as specified in Table given below.

S. N.	Factory Acceptance Test
1	Visual and dimensional checks of all components
2	Tensile test
3	Slip test
4	Galvanising test
5	Wrapping test
6	Hardness test

1.23 Quality Assurance Program

Along with the Bid the Bidder shall furnish quality assurance program of the manufacturer which includes the Quality System and the Quality Plans, which shall include, among others, information to meet the following requirement, failing which the Bid shall be liable for rejection.

i.) The structure of the organization;

ii.) The duties and responsibilities assigned to staff ensuring quality of works;

iii.) The system for purchasing, taking delivery and verification of materials;

iv.) The system for ensuring quality of workmanship;

v.) The quality assurance arrangement shall conform to relevant requirements of ISO 9001;

vi.) Statement giving list of important raw materials, names of manufacturer for the raw materials, list of standards according to which the raw materials are tested, list of tests normally carried out on raw materials;

vii.) List of manufacturing facilities available;

viii.) List of areas in manufacturing process, where stage inspections are normally carried out for quality control and details of such tests and inspections;

ix.) List of testing equipment available with the manufacturer for final testing of equipment specified and the test plant limitation, if any, vis-à-vis the type, special, acceptance and routine tests specified in the relevant standards.

2. Specification for FMS, FODP and Splice Enclosure

This Specification covers the functional & technical specifications of Fiber Management System (FMS), Fiber Optic Distribution Panel (FODP) and Joint Box (Splice Enclosure).

2.1 Fiber Management System (FMS)

Fiber Management System (FMS) or Line Interface Unit (LIU) shall be used at RMU & GO switch locations. These FMS shall be used to connect Fiber optic cable from Manhole / Splice enclosure to the communication equipment.

Indoor FMS Shall be 1U/2U/3U/4U size and rack mountable through sliding into panel. It shall be as per relevant IEC 61754. Outdoor FMS shall be wall mountable or shall be mountable to Ground/Footpath. Outdoor FMS shall also conform IP68 protection and latest relevant IEC standards.

Indoor type FMS shall be installed into the existing Cabinet/Panel of RMU panel. However for outdoor FMS cabinet to be provided along with cabinet and locking arrangement.

Reference: IEC 61754 series. FMS should have following features:

1. Metal base material with powder coating for light mounting.
2. Connectivity available for all type of connector available e.g. SC, LC, FC, ST, E2000 Terminations. There should be arrangement of termination of 96/48/24/12/6 Nos. of fibers
3. It should be mountable in standard 19" rack and of slider type.
4. Shall supplied with all accessories e.g. Cable Ties, mounting ear screw, sleeves, Tissue, Fiber cleaner liquid etc. The FMS shall be manufactured as per latest state of art technology. Body should be of MS steel; powder coating painting (min. 70 micrometer thickness) shall be provided with rust resistance paint.

a. Specifications of Patch Cords

The Patch cords should be confirming to IEC 61754 and IEC 60793-2-50.

2.2 Joint Box

a. Joint Box (Splice Enclosure) and Splicing:

The UGFO and ADSS cables would be required to be spliced at every joint, normally at a distance of every 2 km. Splicing to be for underground cable at Manhole and for ADSS cable on the 33 kV poles. For the ADSS Joint Box, pole mounting structure to be provided along with joint box. Joint box shall be as per compliant with IEC 61753-1 Category A (Aerial) and Category G (Ground),

Telcordia GR-771-CORE or equivalent.

Joint Box shall be universal type that can be placed on underground and overhead locations.

Joint Box shall be suitable to both straight joint and branch joints. Maximum 12 Fibers shall be splices in one splice tray.

For the joint between UGFO and ADSS it will be done preferably on O/H (on the poles).

Manhole shall be placed at around 200m for installation/pulling of UGFO. At these manhole where splicing is not to be done UGFO cable shall kept with 15-meter additional loop for future Telecom purpose.

b. Cable Entry and Sealing Arrangements:

The base shall have a minimum 4 single cable entry ports and one port for express (looped) cable entry. The arrangement shall be provided for terminating looped or express cable by making a suitable necessary provision. All ports shall be sealed and entry ports (sealed) shall be opened as per the requirement. The opening of any port shall not cause any interference to any existing cable. No heat shrink of any type shall be allowed on the cable for sealing. No screws or nut & bolts of any type shall be allowed. The sealing material shall be termite proof. No consumable items shall be required for sealing. The sealing components must be reusable and shall have unlimited shelf life. The sealing arrangements shall be specified along with opening and closing arrangement by the manufacturer and the same shall be tested. It shall be possible to terminate all cables having outer diameter of 20mm (Max.). The joint enclosures shall contain Fiber organizer system where the extra length of Fibers and splices are stored in systematic & secured manner. The method or device for safely routing and securing buffer tube and bare Fiber shall be provided. The joint enclosures shall allow an easy opening and re- closing without degradation in the performance of joint enclosure. Access to the inner junctions shall be possible without damaging the existing cables. The closure must be designed such that no installed cable is disturbed or require re-sealing of the existing cables during installation of additional cables.

c. Holding Arrangements

The box shall provide the following:

1. Holding arrangement and framework for properly securing cable organizers with splice trays.
2. Securing arrangement for holding Fibers.
3. Holding device to hold strength member of Fiber optic cable securely.
4. Any other extra component required for providing strength and reliability to the Joint

Box.

d. Compatibility

All the component and parts used shall be compatible with the optical Fiber cable, Fiber splices and cable components. Their use for long should not result in increase in transmission loss or deterioration in other properties.

e. Marking on body of the Joint box

The following information by marking on Joint box shall be provided:

1. Manufacturer's name & date
2. Type of Joint box
3. Number of Splice organizer cassettes
4. Number of splices per cassette
5. Batch number and serial number.

2.3 Fiber Optic Distribution Panel (FODP)

This section describes the general requirements, type and factory testing requirements of Joint Box for underground optical Fiber cables. At locations requiring the termination of at least one pair Fiber within a cable, all Fibers within that cable shall be connectorized and terminated in FODPs in a manner consistent with the following.

a) FODP shall be provided to accommodate rack mountable 1U (24F) & 2U (48F) FODP Sub rack with Splicing & Patching Trays, with suitable patch cord & Adaptors in Standard 19-inch rack (compliant with IEC 60297) with minimum 42U height.

b) All Fiber optic terminations shall be housed using FODPs provisioned with splice organizers and splice trays. All Fibers within a cable shall be fusion spliced to pre- connectorized pigtails and fitted to the backside of the provided couplings. The pigtails and the Fibers shall be stored and dressed neatly in the provided trays and holders. The pigtails/Fibers shall be numbered using suitable ferrules.

c) Ground lugs shall be provided on all FODP's and the contractor shall properly ground all FODPs. The FODPs shall be properly fixed/grouted to the floor and or with wall with better support. Necessary installation material for fixing the FODP on wall or ground shall be provided by the Contractor.

d) The location of FODPs rack shall be fixed by the contractor, with the Employer's approval.

e) Flexible protection shall be provided to the patch cord bunches going out from FODP to another equipment.

2.3.1 Optical Fiber Connectors

FC-PC type connectors shall be used. Average loss of the FC-PC connectors shall not exceed 0.5dB.

2.3.2 Optical Fiber Splices

Splicing of the optical Fiber cabling shall be minimized through careful planning. It is important that all splicing work be done under clean conditions. All required splices shall be planned to occur at Joint location/manhole. All optical Fiber splicing shall comply with the following:

a) All Fiber splices shall be accomplished through fusion splicing.

b) Each Fiber splice shall be fitted with a splice protection sheath fitted over the final splice.

c) For splicing of each Fiber, every effort shall be made to minimise the bidirectional average splice loss.

d) All splices and bare Fiber shall be neatly installed in covered splice trays.

e) Average bi-directional splice loss at any particular splice shall not exceed 0.1dB but total bi-directional average of all splices in a link shall not exceed 0.05dB.

f) Fiber optic cable service loops as indicated in technical specifications shall be provided.

2.4 Splicing of Fibers in existing Joint Box or FODP

In case it is required to do re-splicing for rectification or splice new cable in an existing Joint Box, above stipulations for splicing shall be applicable. In such conditions, splicing of only few Fibers of the existing cables in the Joint Box with the new cable shall be done. For working in existing Join Box/FODP, the Contractor shall take due care so that the traffic in the balance Fibers is not affected.

2.5 Service Loops

For purposes of this specification, cable and Fiber service loops are defined as slack (excess) cable and Fiber provided for facilitating the installation, maintenance and repair of the optical Fiber cable system.

a) Outdoor Cable Service Loops: At manhole chambers splices are installed with sufficient Fiber optic cable service loops (as mentioned in Technical Specification) such that the recommended minimum bend radius is maintained while allowing for installation or maintenance of the cable to be performed in a controlled environment at ground level. Optical cable service loops (excess cable) shall also be provided at all crossings in manholes (as mentioned in Technical Specification).

b) Indoor Cable Service Loops: At FODPs, Contractor shall provide at least three (3) metres of cable service loop. Service loops shall be neatly secured and stored, coiled such that the minimum recommended bend radius is maintained

c) Fiber Units Service Loops: For all Fiber optic cable splicing, the cable shall be stripped back a sufficient length such that the fan-out of Fiber units shall provide for at least one (1) metre of Fiber unit service loop between the stripped cable and the bare Fiber fan-out.

d) Pigtail Service Loops: Connectorised pigtails spliced to bare Fibers shall provide at least 0.5 metre of service loop installed in the FODP Fiber organizer and at least one (1) metre of service loop to the couplings neatly stored behind the FODP coupling panels.

e) Fiber Service Loops: At least 0.5 metre of bare Fiber service loop shall be provided on each side of all Fiber splices. The bare Fiber service loops shall be neatly and safely installed inside covered splice trays.

2.6 Testing Requirements

a. Type Testing

Type tests for Joint Box:

The Joint Box offered to be supplied should have been type tested as per requirement specified in EC 61753-1 / Telcordia GR-771-CORE or equivalent standard. The contractor shall submit the earlier carried out type test reports for the offered joint box meeting the requirement. List of type tests on joint box are given below:

(i). Water Ingress Test.
(ii). Drop and Topple Test.
(iii). Air Tightness Test.
(iv). Static Load Test.
(v). Impact Test.
(vi). Vibration Test.
(vii). Environmental Cycle Test.
(viii). Salt Spray (Mist) Test.
(ix). (a). Resistance to Aggressive Media Test., (b). Resistance to Stress Cracking Test.
(x). Variation in Attenuation.
(x). Torsion Test.
(xi). Flexure Test.
(xii). Clamping Test.
(xiii). Thermal Aging.
(xiv). Current Surge Test.
(xv). UV Test.

b. Factory Acceptance Testing

Factory Acceptance Tests for Joint Box (Splice Enclosures)

S.N.	Name of test
1	Visual Inspection
2	Tightness (Sealing) Test
3	Static Load test
4	Impact test
5	Axial pull out test
6	Bending test
7	Water ingress test
8	Reopening test

Factory Acceptance Test for FODP

Visual check of Quantities and Specific Component Number for each component of FODP and dimensional checks against the approved drawings.

Factory Acceptance Test for FMS

Visual check of Quantities and Specific Component Number for each component of FMS and dimensional checks against the approved drawings

2.7 Quality Assurance Program

Along with the Bid the Bidder shall furnish quality assurance program of the manufacturer which includes the Quality System and the Quality Plans, which shall include, among others, information to meet the following requirement, failing which the Bid shall be liable for rejection.

i.) The structure of the organization;
ii.) The duties and responsibilities assigned to staff ensuring quality of works;
iii.) The system for purchasing, taking delivery and verification of materials;

iv.) The system for ensuring quality of workmanship;

v.) The quality assurance arrangement shall conform to relevant requirements of ISO 9001;

vi.) Statement giving list of important raw materials, names of manufacturer for the raw materials, list of standards according to which the raw materials are tested, list of tests normally carried out on raw materials;

vii.) List of manufacturing facilities available;

viii.) List of areas in manufacturing process, where stage inspections are normally carried out for quality control and details of such tests and inspections;

ix.) List of testing equipment available with the manufacturer for final testing of equipment specified and the test plant limitation, if any, vis-à-vis the type, special, acceptance and routine tests specified in the relevant standards.