Technical Specifications for Implementation of 5 minute Interface Energy Meters (IEMs) & Automatic Meter Reading (AMR) system, Project on Pan India Basis

September 2026

Rev01

पावरग्रिड
POWERGRID

DISCLAMER

This document, including any extract thereof, is issued solely for the exclusive purpose of bidding against this specification. It shall not be copied, paraphrased, transferred, reproduced, or distributed in any manner or form—whether by photocopying, electronic transmission via the internet, or otherwise—nor shall it be used for any purpose other than that for which it has been specifically issued.

Table of Contents

Chapter 1 — Project 7
1.1 General 7
1.2 Brief of the Project 8
1.3 Country of Origin of Equipment and Services 8
1.4 Scope of work 8
1.5 Specific Exclusions from Contractor's Scope 10
1.6 Location of the Site(s) 10
1.7 Conceptual System Architecture 10
1.8 Schedule of Quantities 11
1.9 Different Chapters of Technical Specifications 11
1.10 Commissioning Material 12
1.11 Specific Technical Requirements 12
1.12 Project Stakeholders and Definitions 13
1.13 Applicable Standards and Regulations 14
Chapter 2 — Interface Energy Meters (IEMs) 15
2.1 Basic Features of Interface Energy Meters 15
2.2 Measurement: 17
2.3 Memory / Storage: 18
2.4 Display 19
2.5 Communication Port 19
2.6 Installation of IEMs 20
2.7 Meter Reading Software at Station PC 20
2.8 Acceptance Tests 21
2.9 Guarantee 22
2.10 Demonstration of Integration of IEMs 22
Chapter 3 — Data Concentrator Units (DCUs) 23
3.1 Role and Function of the DCU 23
3.2 Basic Functions of DCU 23
3.3 Constructional Features of DCU 24
3.4 Communication Ports of DCU 25
3.5 Security Features of DCU 25
3.6 Ethernet Switch 25

3.7 Time Synchronisation Equipment 25
3.8 Technical specifications of substation hardware items 26
Chapter 4 — Automatic Meter Reading (AMR) System 28
4.1 Intent of the AMR System 28
4.2 Network Architecture and End-to-End Data Flow 28
4.3 Scope of Work 28
4.4 Components of the AMR System 29
4.5 Basic Functions of the AMR System 29
4.6 Functional Requirements 30
4.7 AMR System Sizing 34
4.8 Performance Requirements of AMR System 34
4.9 Software requirement of AMR System 34
4.10 Documentation requirements of AMR system 35
Chapter 5 — Control Centre Hardware and Infrastructure 37
5.1 General 37
5.2 Server Hardware - Minimum Requirement 37
5.3 HMI (Workstation) Hardware — Minimum Requirement 39
5.4 Remote Console (All-in-One) 39
5.5 LAN Switch — Minimum Requirement 40
5.6 Network Attached Storage (NAS) 40
5.7 Server Rack Panel 44U 41
5.8 Data Diode & Other Accessories 42
5.9 Processor Terminal -Laptop 43
5.10 Wan Routers At Server Location End 44
5.11 Internal/External Firewall with IDPS For Server Location 45
5.12 Centralized Management Console 54
5.13 Color Laser Printer 54
5.14 Communication Accessories like L2 Switches 55
5.15 Furniture 55
5.16 Time Synchronisation Equipment 56
5.17 Various Power and Communication Accessories 56
5.18 Intrusion Detection & Prevention System 57
5.19 Security Information and Event management (SIEM) 58
5.20 Expandability and Scalability 59
Chapter 6 — Software Requirements and Cyber Security 60

6.1 General Software Requirements 60
6.2 Technical Specifications for Software 60
6.3 Cyber Security — Regulatory Framework 75
6.4 Minimum Cyber Security Measures 75
6.5 Cyber Security Guidelines compliance as per CEA regulations 2026: 77
6.6. Cyber Security Audits 78
6.7 Cyber Security Organisation and Governance 79
6.8 Privacy and Data Protection 79
6.9 Monitoring, Reporting and Vulnerability Management 79
Chapter 7 — Annual Maintenance Contract (Operation, Maintenance & Support Service) 80
7.1 Introduction 80
7.2 Operation 80
7.3 Maintenance support 80
7.4 Maintenance and Support Services Scope 81
7.5 Preventive Maintenance Activity 82
7.6 Resource Deployment, Management & Escalation: 82
7.7 Human Resource Management & Escalation: 83
7.8 Maintenance Audit 83
7.9 Spares Management 84
7.10 Preventive Maintenance, Updates & Upgrades: 84
7.11 Integration of new equipment 85
7.12 Documentation & Reports: 86
7.13 Performance Requirement 86
7.14 Availability Requirements and Penalty during AMC 87
Delay due to any reason not attributable to the contractor shall not be charged and decision of the owner shall be final. 89
7.15 Responsibility Matrix 89
7.16 Other Responsibilities of the Contractor 90
7.17 Review meetings 90
Chapter 8 — Inspection, Testing & Operational Acceptance 91
8.1 General 91
8.2 Quality Assurance and Quality Control Program 91
8.3 Scope of Employer 92
8.4 Inspection and Testing 92
8.5 Testing requirements of AMR system 98

8.6 Dispatch of Material 99
8.7 Site Acceptance Test 99
8.8 Contractor's Maintenance Responsibility till Operational Acceptance 100
8.9 Type Testing & Data Exchange Protocol Testing 100
8.10 Operational Acceptance 101
Chapter 9 — Documents, Drawings and Deliverables 102
9.1 General Documentation Requirements 102
9.2 Design Documents 102
9.3 Software Requirement Specification (SRS) 102
9.4 User Manuals and Training Documentation 102
9.5 Testing Documents 102
9.6 Software and Licence Documentation 102
9.7 As-Built and Historical Documentation 103
9.8 Certificates 103
9.9 Packaging & Protection 103
Chapter 10 — Project Management & Implementation Plan 104
10.1 Introduction 104
10.2 Project Management 104
10.3 Project Schedule 104
10.4 Site Survey and Detailed Engineering 104
10.5 Progress Report 105
10.6 Transmittals 105
10.7 Review Meetings 105
10.8 Outage Coordination 105
10.9 Manpower resources 105
Section 11 — Training and Knowledge Transfer 106
11.1 Training Philosophy 106
11.2 IEM Training 106
11.3 AMR System Training 106
11.4 Software Support Team Training 106
11.5 Knowledge-Transfer Documentation 106
Annexure A — Glossary of Terms and Abbreviations 107
Annexure B — Sample Forms 111
B.1 Weekly AMR Availability Report Form 111
Annexure-C Model Clauses - CEA 2026 guidelines on Cyber Security in Power Sector 112

Chapter 1 — Project

1.1 General

1.1.1 **Preamble**

Power Grid Corporation of India Ltd. (POWERGRID), A Govt. of India Enterprise is responsible for Bulk Power Transmission of electrical energy from various central Govt. Power Projects to various utilities/ beneficiaries and interconnecting regional grids, operating and maintaining the National Electrical Grid of India. It is established with mission of "We will become a Global Transmission Company with Dominant Leadership in Emerging Power Markets with World Class Capabilities by:

1. World Class: Setting superior standards in capital project management and operations for the industry and ourselves
2. Global: Leveraging capabilities to consistently generate maximum value for all stakeholders in India and in emerging and growing economies.
3. Inspiring, nurturing and empowering the next generation of professionals.
4. Achieving continuous improvements through innovation and state-of-the-art technology.
5. Committing to highest standards in health, safety, security and environment.

1.1.2 POWERGRID is executing the work of 5 min Interface Energy Meter along with AMR system on pan India basis

1.1.3 It is the intent of this specification to describe primary features, materials, and design & performance requirements and to establish minimum standards for the work. The specification is not intended to specify the complete details of various practices of manufactures/ bidders, but to specify the requirements with regard to performance, durability and satisfactory operation under the specified site conditions.

1.1.4 The work to be done under this specification shall include all labour, plant, equipment, material and performance of all work necessary for the complete supply, installation, commissioning and AMC. All apparatus, appliances, material and labour etc. not specifically mentioned or included, but are necessary to complete the entire work or any portion of the work in compliance with the requirements implied in this specification is deemed to be included in the scope of contractor.

1.1.5 The bidder may visit all identified ISTS interface points, substations, generating stations, inter-regional points covered under the project to acquaint themselves with the topography, infrastructure and to collate various requirements viz. CT/PT Ratio etc., communication feasibility etc. Also, before proceeding with the installation work the Contractor shall fully familiarize himself with the site conditions and General arrangements & scheme etc. The bidder shall be fully responsible for providing all equipment, materials, system and services specified or otherwise which are required to complete the scope of work and successful commissioning, operation & maintenance of the 5 min IEM and AMR Scheme in all respects. Complete design (unless specified otherwise in specification elsewhere) and detailed engineering shall be done by the Contractor. The following sections would cover the scope of work and other relevant details.

1.2 Brief of the Project

The project envisages the implementation of 5 min Interface Energy Meter (IEM) and Automatic Meter Reading (AMR) System for Inter-State Transmission System (ISTS) Metering points.

The system shall consist of:

- Supply & installation of **IEMs**
- Supply & Installation of Data Concentrator Units (**DCUs)** and associated communication infrastructure at substation level
- Establishment & Commissioning of **AMR system at RLDC/RPC**
- AMC of AMR System

Presently, approx. 14000 no of IEMs are to be integrated in AMR system across all regions at around 1600 locations. Herein, Contractor's scope is for supply of 9500 Nos IEMs (incl. future provision) & balance qty. of AMR compatible existing IEMs is 4500 Nos which are also to be integrated in AMR system.

Eastern Region is presently utilizing an AMR system provided by M/s TCS which is deployed in ERPC premises. Under this project, only existing IEMs shall be replaced with new IEMs. The aforementioned figures are indicative only and BPS to be referred for the exact quantity.

The project includes both **existing operational metering locations (requiring replacement/upgrade of existing meters)** as well as **new interface points**.

The implementation shall be carried out in a **phased and coordinated manner**, ensuring minimal disruption to ongoing grid operations. Installation activities at live substations and generating stations shall be aligned with **approved shutdown schedules and outage coordination procedures**.

The AMR System shall be designed such that all the required hardware, software, and firmware with upgrades satisfy the system requirements and meet service level agreements as specified in this Contract while considering technical obsolescence over the operating life of the system and suitability for future scale up. Contractor is free to decide upon the best solution out of all the available options. However, the entire responsibility of fully functional Interface Energy Metering system shall rest with the Contractor in order to meet the performance levels as given in the Contract. The Contractor shall ensure that the Solution complies with the Applicable Law, technical specifications and other provisions of the Contract.

The detailed scope of the aforesaid work is brought out in subsequent clauses of this section.

1.3 Country of Origin of Equipment and Services

The Bidder shall submit Country of Origin of all items as per Bill of Quantities and any other additional item required for successful completion of the Contract.

1.4 Scope of work

A. The scope of work includes complete design, engineering, supply, installation, integration, testing, commissioning of IEM and AMR systems incl. AMC of AMR system. The scope of work shall include, site survey, planning, design, engineering, manufacturing, supply, transportation & insurance, delivery at site, unloading, handling, storage, installation,

integration, testing, commissioning, training and documentation of the components given below:

i. Conduct detailed site survey and prepare Meter Migration Plan covering CT/PT ratio verification, space assessment, cable routing requirements, communication infrastructure requirements, outage planning and migration schedule.

ii. **Supply, installation, testing and commissioning of** Interface Energy Meters (IEMs) and replacement of existing Meters (as required), Data Concentrator Units (DCUs), communication cables, Ethernet switches, time synchronization equipment (at substation as well as Control Centre Level) and all accessories.

iii. **Supply and installation of network racks, server racks (as applicable) and associated cabling infrastructure**, including power supply arrangements from available source, patch cords, connectors, termination accessories and environmental protection measures wherever applicable for successful operation of the AMR system.

iv. **Establishment, configuration, testing and commissioning of AMR infrastructure**, including servers, storage systems, application software (incl. its upgrades, as & when required), databases, operating systems, web based applications for various applications for monitoring, data sharing purpose to RLDC/SLDC/CTUIL, cybersecurity tools and backup systems required for automated acquisition of 5-minute energy data and 1-minute MW data from Interface Energy Meters.

B. **Generation of automated reports and dashboards** including but not limited to meter availability reports, data availability reports, communication health reports, event and alarm reports, time synchronization reports, validation reports, regional interchange reports and other reports as specified in the Technical Specification.

C. **Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT), cybersecurity audits, performance verification and operational acceptance testing** of all hardware & software supplied under the project.

D. **Submission of all engineering documents, drawings, test reports, operation manuals, maintenance manuals, configuration records and as-built documentation** required for successful operation and future maintenance of the system.

E. **Training of Employer, RLDC, SLDC, Utility and RPC personnel** on installation, operation, maintenance, troubleshooting, administration and utilization of the IEM and AMR systems to ensure efficient, reliable and sustainable operation of the complete metering ecosystem.

F. **AMC Services** for the complete AMR System after successful Operational acceptance of the system.

G. The Scope of Work shall also include, but not be limited to, the following activities for successful implementation, integration, commissioning, operation and maintenance of the 5-Minute IEM, AMR and its interfacing with MDP System:

i. Coordination with the Employer, RLDCs, SLDCs, RPCs, generating stations, transmission licensees, OEMs and other contractors/agencies involved in the project for phased implementation, integration, testing, commissioning and operational acceptance of the complete system.

ii. Restoration and making good of all equipment, panels, control rooms, buildings, structures and facilities modified, disturbed or damaged during project execution by the Contractor or its subcontractors/agencies.

1.5 Specific Exclusions from Contractor's Scope

The following items of work are specifically excluded from the scope of the specifications

a) Space for AMR System at RLDCs/RPCs

b) Auxiliary AC Power Supply source

c) Building, air conditioning systems and other civil infrastructures.

d) Hardware/Software at RLDCs for receiving meter data in .npc format from AMR system.

e) Hardware/Software at SLDCs for viewing 1 min instantaneous MW power flow data from AMR system using secure web browser.

f) Any modification, enhancement, maintenance, troubleshooting or future upgradation of any existing or future RLDC/RPC Meter Data Processing (MDP) system.

g) Laptop/Desktop, Firewall, FOTE at station level.

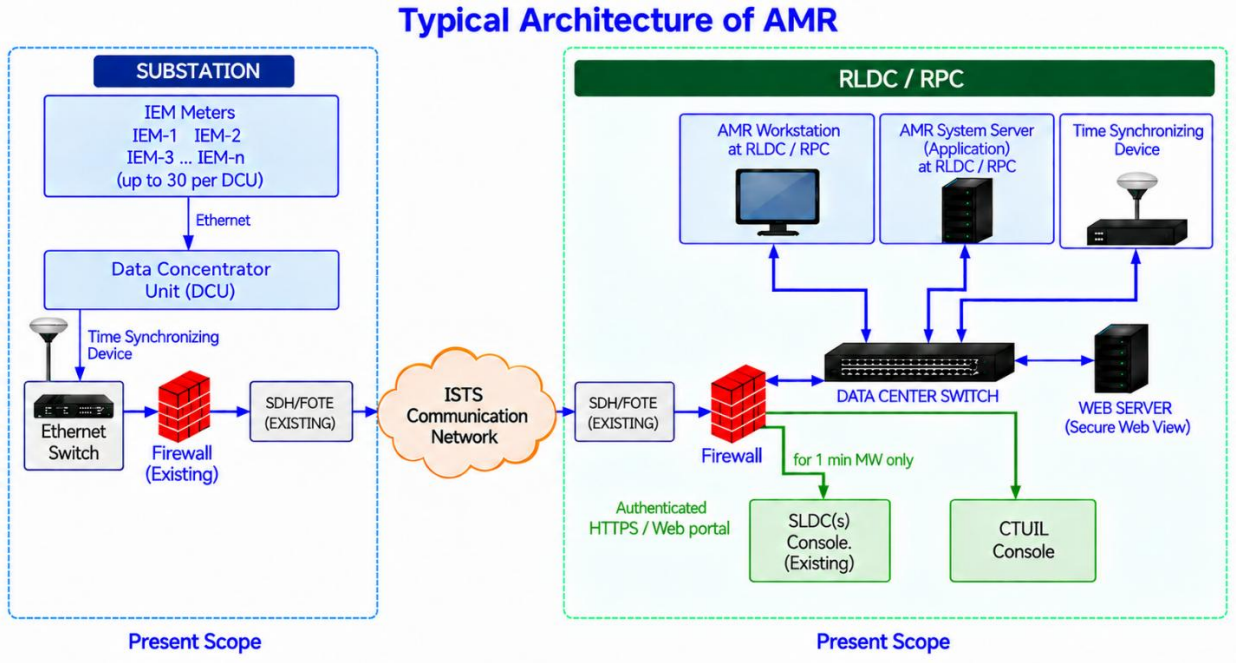
h) Communication between respective ISTS Substation to RLDC/RPC/SLDC/CTUIL, as applicable

1.6 Location of the Site(s)

ISTS substations and generating stations are spread across India. The list of locations is enclosed as Annexure-D.

1.7 Conceptual System Architecture

The AMR system collects both the 5-minute load-survey data and the 1-minute instantaneous MW power-flow data, converts the load-survey data into .npc format, and shares it with the MDP system at the RLDC. The 1-minute MW data is separately made available, through a secure web browser interface, for viewing by SLDCs, and the regional asset data is further shared onward to CTUIL at the national level for consolidated visibility across all regions. A station-level GPS clock, local PC/laptop and firewall support local monitoring, configuration, and time synchronization of the IEMs.



The Contractor shall, during detailed engineering, identify and submit the communication requirements for each location, including required bandwidth, communication interfaces/ports, IP addressing/VLAN requirements, transmission path, latency requirements and any other technical parameters necessary for provisioning and successful operation of the AMR communication links.

1.8 Schedule of Quantities

The requirement of various items /equipment are indicated in Bid price Schedules.

All equipment/items and for which quantities has been given in the BPS shall be payable on unit rate basis. During actual execution, any variation in such quantities shall be paid based on the unit rate under each item incorporated in the letter of award.

Wherever the quantities of items/works are indicated in Lot/Set/LS, the bidder is required to estimate the quantity required for entire execution and completion of works and incorporate their price in respective Bid price schedules. For erection hardware items, Bidders shall estimate the total requirement of the works and indicate module-wise lump sum price and include the same in relevant Bid price schedules. Any material/works for the modules not specifically mentioned in the description in BPS, as may be required shall be deemed to be included in the module itself.

No cost compensation shall be considered on account of "Set/LOT/LS" items in case of number of IEMs / Substations / AMR Control Centres specified in section project remains unchanged

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. Item which explicitly may not appear in various schedules and required for successful commissioning of substation shall be included in the bid price and shall be provided at no extra cost to Employer.

1.9 Different Chapters of Technical Specifications

For the purpose of present scope of work, technical specification shall consist of following chapters and they should be read in conjunction with each other.

S.	List of Chapter of TS
1.	Chapter 1: Project

2.	Chapter 2: Interface Energy Meters (IEMs)
3.	Chapter 3: Data Concentrator Units (DCUs)
4.	Chapter 4: Automated Meter Reading (AMR) System
5.	Chapter 5: Control Centre Hardware and Infrastructure
6.	Chapter 6: Software Requirements, Database and Cyber Security
7.	Chapter 7: Annual Maintenance Contract (Operation Maintenance & Support Services)
8.	Chapter 8: Inspection, Testing & Operational Acceptance
9.	Chapter 9: Documents, Drawings and Deliverables
10.	Chapter 10: Project Management & Implementation Plan
11.	Chapter 11: Training and Knowledge Transfer

In case of any discrepancy between SECTION-PROJECT and other technical specifications on scope of works, SECTION-PROJECT shall prevail over all other sections.

1.10 Commissioning Material

Any material required for commissioning purpose shall be arranged by the Contractor without any financial implication to POWERGRID. The unutilized material, if any, is brought for commissioning purpose may be taken back by the contractor.

After completion of the work, Contractor may take back all the unutilized material brought for completion of scope of work at his own cost and shall make the work area properly cleaned.

1.11 Specific Technical Requirements

1.11.1 Communication Media

The existing ISTS Communication network shall be utilized for AMR system for communicating between substation DCU, RLDC, RPC, SLDC and CTUIL.

The Contractor shall be responsible for all AMR-side equipment, interfaces, patching up to the designated FOTE/interface point and associated testing. The existing ISTS communication backbone shall remain under the operation, control and maintenance of its designated owner.

1.11.2 Establishment of AMR System infrastructure at RLDC / RPC end

The Contractor shall ensure that the AMR system infrastructure at the RLDC/RPC end, including all associated hardware, software, databases, communication interfaces, and data-sharing interfaces with the RLDC's Meter Data Processing (MDP) system, is established, tested, and commissioned prior to commencement of commissioning activities for Interface Energy Meters (IEMs) and associated field infrastructure such as DCUs at substations. This is essential to facilitate seamless onboarding of both existing and newly commissioned metering infrastructure and to ensure availability of metering data at the RLDC/RPC end from Day-1 of meter commissioning for energy accounting, data validation, and monitoring purposes. Accordingly, commissioning of the RLDC/RPC AMR infrastructure shall be treated as a prerequisite milestone for commencement of substation-level meter commissioning activities.

1.11.3 Integration of IEMs with existing AMR of Eastern Region

Eastern Region is presently utilizing an AMR system supplied by M/s TCS which is deployed in ERPC premises. Under this project, existing IEMs shall be replaced with new IEMs. IEMs under the present scope project shall be integrated in existing AMR. Existing AMR OEM shall integrate these IEMs in their AMR system. However, necessary support for integration of IEM in AMR system shall be provided by Contractor.

1.11.4 Integration of existing AMR compatible Meters in New AMR System

AMR-compatible Interface Energy Meters (IEMs) have already been installed, or are under installation, by various utilities across different Regions. These meters shall also required to be integrated with the AMR system being implemented under present scope. The Region-wise details of such meters is given in BPS.

1.11.5 Exit Management

Upon completion or termination of the contract, the Contractor shall provide complete support for transfer of system configuration, databases, reports, licenses, documentation and operational records to the Employer or successor agency without interruption of AMR services.

1.11.6 Annual Maintenance Contract (Comprehensive)

The contractor shall have to maintain the system and provide comprehensive maintenance services as defined in relevant Chapter after operational acceptance by Employer.

1.12 Project Stakeholders and Definitions

Term	Definition
Employer	The implementing agency to whom the work of establishing the IEM/AMR system is assigned
Owner	The entity in whose premises the meter is installed, as defined under the CEA (Installation and Operation of Meters) Regulations.
Contractor / Bidder / Vendor / Supplier	The successful bidder engaged to design, supply, install, test, commission, and support the IEM/DCU/AMR system under this specification.
CEA	Central Electricity Authority, Ministry of Power, Government of India.
NPC Division	National Power Committee Division of CEA, which convenes and services the Joint Committee.
RPC	Regional Power Committee (NRPC, WRPC, ERPC, SRPC, NERPC).
RLDC / NLDC	Regional Load Despatch Centre / National Load Despatch Centre.

Term	Definition
SLDC	State Load Despatch Centre.
CTUIL	Central Transmission Utility of India Limited
GRID-INDIA	Grid Controller of India Limited, operator of the National/Regional Load Despatch Centres.
IEM	Interface Energy Meter at ISTS Interface points
DCU	Data Concentrator Unit — the substation-level device interfacing IEMs with the AMR system.
AMR	Automatic Meter Reading system, located at RLDC/RPC.
MDP	Meter Data Processing system, located at RLDC, used for validation, computation and energy accounting.
SDH	Synchronous Digital Hierarchy
ISTS Communication Network	Unified Load Despatch and Communication network — the power-sector-owned WAN connecting substations to RLDCs/SLDCs.
DSM	Deviation Settlement Mechanism.

1.13 Applicable Standards and Regulations

- CEA (Installation and Operation of Meters) Regulations, 2006 and amendments thereof.
- IS 14697 — AC Static Transformer Operated Meters for Active and Reactive Energy (Class 0.2S/0.5S), and amendments.
- IS 15959 — Data Exchange for Electricity Meter Reading, Tariff and Load Control, and amendments.
- CEA Cyber Security regulation 2026
- IEGC 2023 and its amendments thereof
- ISO/IEC 27001 for information security and privacy management.
- ITU-T G.707/G.783 series for SDH transmission equipment or latest
- Relevant IEC standards for metering, communication protocols (DLMS/COSEM) and electromagnetic compatibility.

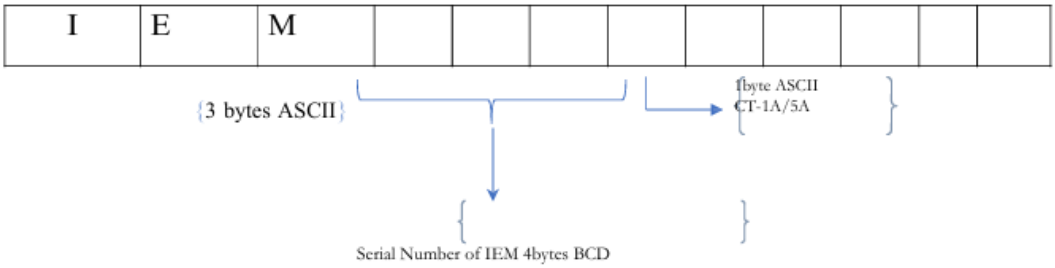
Chapter 2 — Interface Energy Meters (IEMs)

The Interface Energy Meter shall be designed for continuous unattended operation in extra-high voltage substations under severe electrical and environmental conditions.

2.1 Basic Features of Interface Energy Meters

i. The energy metering system specified herein shall be used for tariff metering for bulk, inter-utility power flows, in different States of India. Projection mounted type, Static composite AC 3-ph 4 wire meter shall be installed at interface points as a self-contained device for measurement of Voltage (V), Frequency (f), Active (Wh) and Reactive (VArh) energy exchanged in each successive user defined (5 min/15 min) time block. Meter time block shall be reconfigurable at site for change of time block as specified by CERC. All meters shall be compliant to CEA (Installation and Operation of meters) Regulations 2006 and its amendments & IS 15959 and its amendments.

ii. Each meter shall have a unique identification code, which shall be marked permanently on its front, as well as in its memory. All meters supplied to as per this specification shall have their identification code starting with "IEM". "IEM" shall be followed by an eight-digit running serial number, further followed by a "A" and "B" for the use with CT secondary of 1A and 5A respectively. This shall be mutually agreed between the buyer and the vendor.



iii. The meters shall be DLMS protocol compliant and shall be suitable for communication with external device like modem, DCU, etc. which shall be able to communicate with AMR system for remote data transfer.

iv. Auxiliary Supply to IEM- The meters shall normally operate with the power drawn from the VT secondary circuit (line-to line voltage of 110V i.e. Vref); provided that there shall be provision to operate the meters from AC (240V AC) and DC (110V/ 220V DC) auxiliary power supply. Necessary isolation and/or suppression shall also be built-in as per IS 14697 and its amendments, for protecting the meters from surges and voltage spikes from extra high voltage switchyards. The reference frequency shall be 50Hz. Also, the meter shall be suitable of ±10% tolerance for AC/DC supply.

v. Variation in CT/PT - The meters shall safely withstand the usual fluctuations arising during faults etc. In particular, VT secondary voltages 115% of Vref applied continuously and 190% of Vref for 3.0 seconds, and CT secondary of Iref applied continuously and 30 times of Iref applied for 0.5 seconds shall not cause any damage to or maloperation of the meters.

vi. The meters shall continue to function for the remaining healthy phase(s), in case one or two phases of VT supply fails. In case of a complete VT supply failure, the computation of average values shall be calculated and recorded along with the time only for the period during which the VT supply was available in configured time block. However, the integrated parameters (active/reactive energy) shall not be affected and recorded as actuals

vii. The total burden imposed by a meter for measurement and operation shall be defined as per IS 14697 and its amendments. An automatic backup for continued operation of the meter's calendar- clock, and for retaining all data stored in its memory, shall be provided through a long- life battery. The meters shall be supplied duly fitted with the batteries, which shall not require to be changed for at least 10 years, as long as total VT supply interruption does not exceed two years.

viii. The meters shall fully comply with all stipulations in IS 14697 and its amendments except those specifically modified by this specification. The reference ambient temperature shall be 27 Deg C.

ix. Each meter shall be provided with optical test output device (visual), as per IS 14697 and its amendments for checking the accuracy of active energy (Wh) measurement. The preferred pulsing rate is twenty (20) per Wh for CT sec-1A and four (4) per Wh for CT sec –5A.

x. Exception Management- The three line-to-neutral voltage shall be continuously monitored and in case any of these falls below defined threshold (80% of Vref), meter shall have suitable indication on LED/ LCD. The meter shall also have provision for low voltage event logging in meter memory in case of any phase voltage going below a defined threshold. The time blocks in which such a voltage failure occurs/persists shall also be recorded in the meter's memory with a symbol"*" if 3 Phase RMS voltage applied to the IEM is in between 25% to 80% of Vref and if Voltage is less than 25% of Vref, meter should record Zero voltage symbol "Z".

xi. Time Accuracy - Each meter shall have a built-in calendar and clock, having an accuracy of 10 seconds per month or better. The calendar and clock shall be correctly set at the manufacturer's works. The date (year-month-day) and time (hour-min.-sec.) shall be displayed on the meter front on demand. Meter shall have the intelligence to synchronize the time locally from dedicated time synchronizing equipment as per project or remotely from AMR system through software. All clock correction information (GPS time, meter time at receipt of synchronization signal) shall be registered in the meter's memory, suitably shown in the meter data report and the also shall be shared to AMR system whenever the time difference between meter time and GPS clock time at the time of synchronization found more than 1 sec.

xii. The IEMs shall be supplied with latest version of Firmware. A touch key or push button shall be provided on the meter front for switching on the display and for changing from one indication to the next

xiii. Standard Raw data format for .NPC conversion:

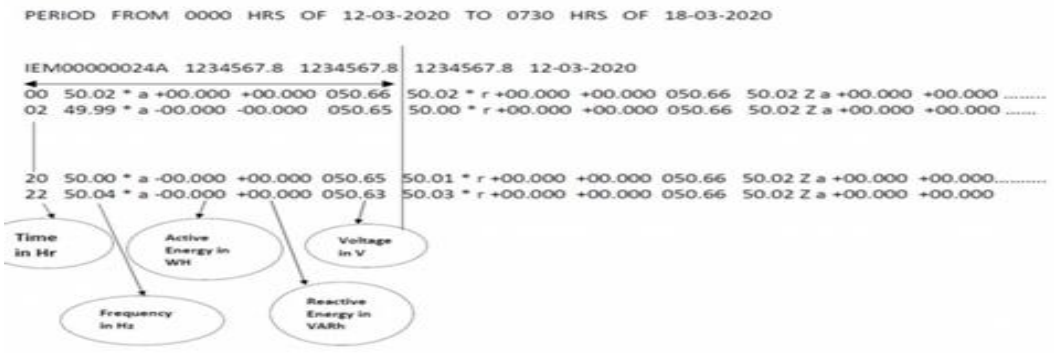


Fig 2 – Standard raw data format of IEM

There are 4 values in one 5 min time block. The first row shall contain the meter data for 2 hours, i.e. 24 time blocks, 00 hrs to 02:00 hrs. Similarly the 2nd row shall contain the data for the next 2 hours and henceforth.

xiv. Accuracy of IEMs under transients, frequency variations, voltage variations, unbalance, harmonics. Electromechanical influence and reverse phase rotation etc. shall be maintained as per IS 14697 and its amendments.

xv. Self-Diagnostic Feature: The IEMs shall be capable of performing complete self-diagnostic check to monitor all circuits for any malfunctioning to ensure proper functioning of the meter all the time. The meter shall have indications for unsatisfactory/ malfunctioning of the following.

a. Non volatile memory
b. RTC battery

The said malfunctioning should be flagged as LED indication on the front of the IEMs and at station PC (existing) through DCU as alarm/indication and also at AMR system at RLDCs/RPCs

xvi. Constructional Features

a. The meters shall be supplied with compact and sturdy, metallic or moulded cases of non-rusting construction and/or finish. The cases shall be designed for simple mounting on a plane, vertical surface such as a control/relay panel front. Terminals shall have a suitable construction with barriers and cover, to provide a secure and safe connection of CTs and VTs leads through stranded copper conductors of 2.5 sq. mm. size.
b. All meters of the same model shall be totally identical in all respects except for their unique identification codes. They shall also be properly sealed and tamper evident, with no possibility of any adjustment at site as per IS 15959 (and its amendments) & CEA (Installation and Operation of meters) Regulations 2006 (and its amendments).
c. The meters shall safely withstand, without any damage or mal operation, reasonable mechanical shocks, earthquake forces, ambient temperature variations, relative humidity, other external factors etc. in accordance with IS- 14697(and its amendments) & CEA (Installation and Operation of meters) Regulations 2006 (and its amendments).
d. They shall have at least IP51 category dust tight construction, and shall be capable of satisfactory operation in an indoor, non-air-conditioned installation & outdoor installation in a panel.
e. The meters shall have built-in facility (e.g. test links in their terminals) for in-site testing.
f. The meter shall be immune to external influences like magnetic induction, vibration, electrostatic discharge, switching transients, surge voltages, oblique suspension and harmonics and necessary tests shall be carried out in accordance with relevant standard.

xvii. Data Security: Data security shall be as per

a. IS 15959 (three layers of security) and its amendments,
b. Cyber Security guidelines/regulations issued by MoP, GoI, CEA & CERC time to time &
c. The technical standards for communication system in Power Sector laid down by the Authority (CEA).

2.2 Measurement:

a. The active energy (Wh) measurement shall be carried out on 3-phase, 4-wire principle, with an accuracy as per class 0.2S as specified in IS 14697.

b. The meter shall provide the instantaneous active power flow data (W) sent out from the substation busbars in each successive 1 min block, and send the MW value upto two decimal place to AMR control centre.
c. The meter shall compute the net active energy (Wh) sent out from the substation bus bars during each successive time block, and store it in its memory up to two decimal place. Further Wh data in .NPC/output report shall be truncated upto two decimal.
d. The meter shall count the number of cycles in VT output during each successive time block, and divide the same by time (in sec) to arrive at the average frequency. The least count of the frequency data shall be 0.01 Hz. The frequency data shall be stored in the meter's memory in Hertz up to two decimal. Further frequency data in .NPC/output report shall be truncated upto two decimal.
e. The meter shall continuously compute the average of the RMS values of the three line- to-neutral VT secondary voltages as a percentage of 63.51 V, and display the same on demand. The accuracy of the voltage measurement/computation shall be at least 0.5%. The voltage data shall be stored in the meter's memory in volts (line voltage e.g. 110V) up to second decimal. Further voltage data in .NPC/output report shall be truncated upto two decimal.
f. The Reactive energy (VARh) measurement shall be carried out on 3-phase, 4- wire principle, with an accuracy of 0.2S similar to Wh measurement. The meter shall compute the net Reactive energy (Net VARh=(VARh Export- VARh Import)) sent out from the substation bus bars during each successive time block, and store it in its memory up to second decimal. It shall also display on demand the net VARh sent out during the previous time block. Further VARh data in. NPC/output report shall be truncated up to second decimal.
g. The meter shall also integrate the reactive energy (VARh) algebraically into two separate registers, one for the period for which the average RMS voltage is above 103.0%, and the other for the period for which the average RMS voltage is below 97.0%. The current reactive power (VAR), and cumulative reactive energy (VARh) readings of the two registers (>103% and <97%) shall be displayed on demand. The voltage range of +/- 3% (i.e 97 to 103) shall be configurable as and when required in future. The readings of the two registers at each midnight shall also be stored in the meter's memory. When reactive power is being sent out from substation bus bars, VAR display shall have a plus sign or no sign and VARh registers shall move forward. When reactive power flow is in the reverse direction, VAR display shall have negative sign and VARh registers shall move backwards. Generally, the standard PT ratios are 132 kV/110 V, 220 kV /110 V, 400 kV /110 V and 765 kV / 110 V. However, at the time of commissioning the vendor may confirm the same from site (authorized sign) and configure the meter accordingly to ensure correct recording of reactive energy.
h. For reactive power (VAR) and reactive energy (VARh) measurements, IS14697 shall be complied with. The accuracy of measurement of reactive energy shall be as per the standard.
i. Further, the meter shall continuously integrate and display on demand the net cumulative active energy sent out from the substation bus bars up to that time. The cumulative net Wh reading at each midnight shall be stored in the meter's memory. The register shall move backwards when active power flows back to substation bus bars.
j. Errors for different power factors shall be as defined in IS14697 and its amendments.
k. The harmonics shall be filtered out while measuring Wh, V and VARh, and only fundamental frequency quantities shall be measured/computed.

2.3 Memory / Storage:

i. Each meter shall have a non-volatile memory in which the following shall be automatically stored:
   a. Average frequency for each successive time block, in Hertz up to 2 decimal truncation.

b. Net Wh transmittal during each successive time block, up to second decimal, with plus sign for active power sent out from station busbars and minus sign for active power received into the busbars
c. Net VARh transmittal during each successive time block, up to second decimal with plus sign for reactive power sent out from station busbars and minus sign for reactive power received into the busbars.
d. Cumulative Wh transmittal at each midnight, in eight digits including one decimal.
e. Cumulative VARh transmittal for voltage high condition, at each midnight in eight digits including one decimal.
f. Cumulative VARh transmittal for voltage low condition, at each midnight, in eight digits including one decimal.
g. Average RMS voltage for each successive time block upto 2 decimal truncation.
h. Date and time blocks of failure of VT supply on any phase, as a star (*)/ (Z) mark.

ii. The meters shall store all the above listed data in their memories for a period of minimum fifteen (15) days.
iii. 1min instantaneous MW power flow data shall be sent to AMR system without storing data in meter memory.

2.4 Display

Each meter shall have digital display for indication of the following (one at a time), on demand:

a. Meter serial no.: IEM12345678A or IEM12345678B
b. Date (year month day /yyyy mm dd): 20160311 d
c. Time (hour min sec /hh mm ss): 195527 t
d. Cumulative Wh register reading: 1234567.8 C
e. Average frequency of the previous time block: 49.89 F
f. Net Wh transmittal during the previous block with +/- sign: - 28.75 E
g. Net VARh transmittal during the previous block with +/- sign:- 18.75 R
h. Average % Voltage: 99.2 U
i. Reactive power (VAR): 106.5 r
j. Voltage - high VARh register reading: 1234567.5 H
k. Voltage - low VARh register reading: 1234567.4 L
l. Low battery indication
m. The three line-to-neutral voltages shall be continuously monitored and in case any of these falls below 80 %, then preferably, the corresponding flashing LED provided on meter's front shall become steady. They all shall go off if all three voltages fall below 80 %. The LED shall automatically resume flashing when all VT secondary voltages are healthy again.
n. The two VARh registers (x and xi) shall remain stay-put while VT supply is unhealthy. Navigation keys to be provided at the meter front plate to navigate the display menu.

Note: These are typical minimum requirements as per CEA metering regulation and shall be finalized during detailed engineering.

2.5 Communication Port

a. All the meters shall have at least three ports. One of these ports shall be compatible for Ethernet traffic through which all the data stored in the meter's memory shall be transferred to DCU. The data between Meter and DCU is exchanged using Ethernet standard frame structures defined in IS15959. The second port shall be front Optical port suitable for admin

access / meter configuration/ local data downloading. The admin port is password protected for access and the meter configuration is to be done through admin port using Laptop and optical to USB convertor. Optical to USB convertor cable of suitable length to be supplied at every location. (Third port shall be Rs485 as spare and shall be used for meter data access in case of any eventuality. One number RS485 to USB convertor cable of suitable length to be supplied at every location.

b. All the three ports shall be able to transmit data simultaneously.

c. The galvanic isolation of these ports is such that no external electrical induction on cable degrades the performance of the meter. Meter data shall be tamper-proof.

d. Data collection on any local laptop/PC shall be possible by installing data collection software. It shall be ensured that data transfer through Optical to USB interface shall be unidirectional only i.e. from Meter to external storage device in an authentication process.

2.6 Installation of IEMs

Other activities as mentioned below to be carried out to ensure successful installation and commissioning:

a. Dismantling, removal and handing over existing Interface Energy Meters (IEMs), wiring, communication cables and other redundant metering infrastructure, wherever applicable to owner utility of that substation.

b. Primarily installation of New IEM is to be carried out in place of existing IEM only, hence, necessary cabling shall be already available. However, if there is requirement of installation at new location in same / nearby panel, suitable wiring shall be in Contractor's scope.

c. Contractor to carry out Installation, testing and commissioning of new IEMs, DCUs and associated communication equipment along with all required accessories such as CT/PT wiring, terminal blocks, lugs, glands, ferrules, connectors and patch cords etc. All installation, cable laying and termination work shall be carried out in accordance with Employer's guidelines, applicable standards and safety requirements. Where cables or related materials are provided by the Employer, laying, installation, termination and commissioning of the same along with associated accessories shall be in the Contractor's scope without any additional cost.

d. All associated minor structural and miscellaneous works required for dismantling existing equipment and installation of new metering, communication and networking infrastructure shall be carried out by the Contractor. The scope shall include fabrication and installation of mounting arrangements, supports, cable trays, brackets, equipment racks, communication cabinets, drilling, grouting, trenching, sealing, restoration and all incidental work necessary for successful installation, integration and commissioning of the IEM, AMR system. Any modifications required in existing panels, control rooms or communication facilities for accommodating new equipment shall also be included in the Contractor's scope.

2.7 Meter Reading Software at Station PC

Software based on Windows-10 & its higher version Operating System for Local communication with meters shall be supplied for viewing/ downloading the meter data, status, alarms etc. without any extra cost and shall be considered as integral part of the metering equipment. The software shall be capable to do the following tasks primarily:

a. Downloading of 5 min load survey data in case failure of data reading through AMR

b. Clock adjustment of meters

Installation agency of meter as per CERC/CEA metering regulation shall facilitate/install the meter reading software at substation PC for viewing/downloading the meter data at the time of meter installation in existing station PC or laptop.

Meter reading software of related make meters shall be made available by the OEM with installation manual. (Any updates, patch updations or software updations etc. shall be properly covered/addressed under the warranty for removal of difficulties faced by the users.)

Encryption key for conversion of encrypted raw data into readable format from the meter vendors would be provided to implementing agency and Grid-India/RLDCs.

2.8 Acceptance Tests

All equipment, after final assembly and before dispatch from manufacturer's works, shall be duly tested to verify suitability for supply to the Owner**. Testing of meters shall be carried out in line with CEA (Installation and Operation of meters) Regulations 2006 (and its amendments) and relevant standards.

i. Type Test & Routine Test for IEM-

a. The meters shall be subjected to the complete range of type tests & routine tests as per IS14697 and IS15959 and their amendments and other applicable standards, after final assembly
b. Type test conducted once shall be valid for 5 years for the same model. Copy of Test certificate shall be submitted to Employer.
c. The type tested meters shall not be supplied/installed. The Bidder shall arrange all type testing specified above, and bear all expenses for the same.
d. Type tests shall be certified or performed by NABL accredited laboratories as per CEA (Installation and Operation of meters) Regulations 2006 (and its amendments) and relevant standards using data sheets and test procedures that have been approved by the Employer.

ii. Factory Acceptance Test (FAT)-

The FAT shall be conducted according to the FAT Test Plan and Test Procedure approved by Employer and shall cover the following Tests as per IS 14697 as a minimum-

1. Test of Starting Condition
2. Test of No-Load Condition
3. Test of Meter Constant
4. Insulation Resistance Test
5. AC High voltage test
6. Test of Power Consumption
7. Test of Limits of Error
8. Test of Repeatability of Error
9. Functional Test i.e. i) Voltage Variations, Frequency Variations, c) Phase Sequence Reversal
10. ABT features verification i.e. a) Test for reactive high register when V> 103% Vref & for reactive low register when V<97% Vref.
11. Communication Test through Ethernet port, RS 485 and Optical admin port
12. Cyber security test as per the CEA Regulations on Cyber security in power sector 2026
13. Downloading of Meter data using communication –
    a. Downloading Meter Data from the Meter(s) to PC via admin Optical port.

b. Downloading meter data to DCU through Ethernet port. IEMs along with convertor, Optical Switch, DCU shall be integrated with the PC for demonstration.
c. Downloading Meter Data from the Meter(s) to PC via RS 485 port

14. Testing of Time Synchronization
15. Visual Inspection- To verify that the system to be delivered has all required components and is properly configured. Visual inspection shall verify acceptable workmanship and that all equipment, including cables and connectors, are appropriately labelled.

A procedure/schedule for the above demonstrations shall be submitted to the employer for approval. Copy of Test certificate shall be submitted to Employer.

2.9 Guarantee

i. The IEM shall be guaranteed for a period as per relevant clause of SCC from the date of Operational Acceptance.
ii. The guarantee would include repair, replacement and part material replacement cost. Transportation of defective material from respective site to contractor's centre shall be in owner's scope whereas from contractor's centre to site shall be carried out by contractor. Necessary insurances shall be ensured by respective parties.
iii. Meter software, if upgraded by OEM should be supplied free of cost. Also, patch updations or software updations, software problem etc. should be addressed free of cost.
iv. Meters which are found defective/inoperative at the time of installation or become inoperative/defective within the guarantee period, the same shall be attended by service engineer from contractor's regional service center within ten days of receipt of report concerned owner utility. Service engineer shall repair the defective meter, upon unable to rectify, the same shall be replaced with spare meter borrowing from Owner. The spare meter shall be replenished with new meter by OEM in another one week time without any cost implication.
v. Copy of warranty certificate shall be submitted to employer.

2.10 Demonstration of Integration of IEMs

It is mandatory to demonstrate the capability of meter to capture 5 min Load survey data and 1 min instantaneous power flow data along with compatibility with DCU in DLMS protocol before mass fabrication. Further, Contractor shall provide the demonstration of complete system i.e. integration of IEM with AMR system as per TS. For this purpose, successful bidder shall arrange necessary facilities like meter reading software, networking equipment and associated hardware etc.

****

Chapter 3 — Data Concentrator Units (DCUs)

3.1 Role and Function of the DCU

A Data Concentrator Unit (DCU) installed at each station will act as interface between IEMs and AMR system at RLDCs/RPCs. DCU shall collect data from energy meters (atleast 30 IEMs/DCU) and send the same to AMR system at RLDCs/RPCs. DCU shall also report diagnostic information of the energy meters to AMR System. The DCU shall be multi- vendor interoperable to support communication of different make IEMs with Centralized AMR system.

3.2 Basic Functions of DCU

i. **Acquiring 5 min load survey data and 1 min instantaneous MW power flow data from IEMs.** :- DCUs shall be connected with energy meters through Ethernet to Optical convertors (good quality) in the switchyard & Optical Switches in between. Connection to the IEMs shall be firm and secure from any unintended disconnection.

ii. **Providing meter data to AMR central server at RLDC/RPC:-** DCUs shall query meter data from IEMs and transfer the same to AMR system based on the command received from AMR control centre. Command may be for one time demand of data or it may be on cyclic basis as defined in Task Scheduler application (to be finalized in design document during engineering phase).

AMR system takes the updated Database from these DCUs and create suitable Database in its memory at Control Centre. DCU shall be able to query data from all or selected energy meters for the selected period based on the command from AMR system. DCUs shall be able to read meter data from all make of energy meters supplied as per this Technical Specification as well as existing AMR capable IEMs.

Each meter has a unique identification number and each meter location has unique identification code. DCUs shall collect data as per TS from IEMs and transfer the same to AMR system. As DCU shall function on read and forward philosophy for IEM data, no storage is envisaged in the DCUs for meter data.

iii. **Acquiring status and alarm from energy meters:-** DCUs shall acquire connected IEM details like meter identification number, make etc. whenever it's powered on. Any meter change activity like meter number etc. shall be reported to AMR system immediately.

DCUs shall be self-monitoring for alarm like power failure, communication disconnection, and disconnection from energy meters and report the same to AMR system immediately and also to local computer.

DCUs shall have non-volatile memory for storing details of IEMs duly time stamped, details of connected meters like make, meter number, status change. Non-volatile memory should be able to store such details for at least one month in round FIFO buffer.

iv. **Providing IEM data to local computer at substation:-** Software based on Windows-10 & its higher version Operating System at existing local computer at substation shall be supplied for viewing/ downloading the meter data, status, alarms etc. DCU shall be connected to the existing PC having the software for viewing/ downloading the meter data, status, alarms etc. Local PC shall be able to query meter data from selected or all IEMs. All communication between local computer and DCU/IEM shall be password protected and only limited to restricted user.

The software shall be capable to do the following tasks primarily.

- Downloading of 5 min load survey data through DCU
- Clock adjustment of meters from local station GPS
- Receiving of all alarms & events from DCU
- Generation of Log sheet/incident report

Station PC shall be arranged by respective site/ utility.

v. **Time synchronization of IEMs, either from dedicated AMR GPS installed at site or from control center AMR Software (MDAS):-** DCU shall have the intelligence to synchronize the IEM clock time. Input signal to DCU shall be from AMR system GPS clock. If AMR system clock synch signal is not available to DCU, DCU will get GPS clock reference from dedicated AMR GPS installed at Substation end. DCU shall function as SNTP servers to the IEMs and SNTP clients to AMR system SNTP servers.

vi. **Display:-** Each DCU shall be provided with indicative LEDs for monitoring of Power supply status, Healthiness of DCU.

vii. DCU shall support remote configuration from AMR control centre. DCU shall accept only digitally signed files for Configuration updates, Firmware updates, package updates, License updates & Patch updates. Only root user shall have the rights to modify/delete DCU logs.

viii. Each DCU shall be capable to connect at least 30 IEMs for polling on ethernet port over DLMS protocol without any delay in Data Collection process. Accordingly, additional DCU shall be provided in case the number of IEMs becomes more than thirty at any substation.

ix. The data exchange & encryption shall be as per the IS 15959 :2011 standard and its amendments.

3.3 Constructional Features of DCU

i. DCU shall be a self-contained, stand-alone, tamper proof sealed box with necessary ports for external connection.

ii. DCU shall not have any removable parts such as a hard disk, to ensure smooth and reliable operation for long term.

iii. All external connections to DCU should be secure so as to avoid accidental disconnection.

iv. The DCU shall be powered from the station battery supply rated at 220V/110V DC supply. Exact DC voltage at each station shall be collected by the contractor during site survey prior to detailed engineering stage. Contractor shall provide DCUs accordingly.

v. DCU shall be able to operate in environment with temperature up to 50ºC and humidity up to 90% without any significant effect on its performance.

vi. DCU shall have surge protection and filtering to provide protection against voltage spike if any.

vii. The mechanical design and construction of each unit sub-assembly shall be inherently robust and rigid under various conditions of operation, adjustment, replacement, storage and transport.

viii. DCUs shall also withstand, without any damage or mal-operation, reasonable mechanical shocks, earthquake forces, ambient temperature variations, relative humidity etc. They shall have at least IP-51 category dust tight construction and shall be capable of satisfactory operation in an indoor, non-air-conditioned installation.

3.4 Communication Ports of DCU

i. Minimum One number Ethernet port & Two RJ 45 ports to connect the meters, local GPS clock, station PC/Laptop through optical switch.

ii. DCU shall be capable of sending 5 min load profile data as well as 1 min instantaneous MW power flow data simultaneously to AMR system.

3.5 Security Features of DCU

i. Authentication & Access Control

- Role-Based Access Control (RBAC)
- User authentication using passwords, certificates, or centralized authentication servers
- Secure remote management access (SSH/HTTPS)

ii. Encryption

- DLMS/COSEM Security Suite supporting cryptographic algorithms
- TLS 1.2 or higher for communication with AMR

iii. Firmware & Software Security

- Authenticated remote firmware upgrades
- Digitally signed firmware validation before installation
- Secure boot mechanisms
- Rollback protection to prevent loading older vulnerable firmware versions

iv. Logging & Audit Trails

- Security event logging
- User activity logs
- Communication failure logs

Tamper and configuration change records

3.6 Ethernet Switch

i. 24 ports Industrial grade layer 2 Ethernet Switch, 12 number 10/100/1000 MBPS RJ 45 ports & 4 numbers 1/10G FO Port at Substation Control room to connect IEMs to DCU.

ii. Industrial grade layer 2 Ethernet Switch with required RJ 45 ports and FO ports at Switchyard location to convert electrical data to optical.

iii. Switch shall be suitable for 220V / 110V DC power supply with rack or DIN or panel mountable hardware

iv. Minimum 2 no spare ports in each switch shall be ensured during implementation.

Note- Number of ethernet switch at each station shall be as per requirement during detailed engineering.

3.7 Time Synchronisation Equipment

i. The Time synchronization equipment shall receive the coordinated Universal Time (UTC) transmitted through Geo Positioning Satellite System (GPS) / NAVIC and synchronize equipment to the Indian Standard Time in a substation.

ii. Time synchronization equipment shall include antenna, all special cables and processing equipment etc.

iii. It shall be compatible for synchronization of IEM & DCU, at a substation through individual port or through Ethernet

iv. Equipment shall operate up to the ambient temperature of 50 degree centigrade and 80% humidity.
v. The synchronization equipment shall have 1.5 micro-second accuracy. Equipment shall give real time corresponding to IST (taking into consideration all factors like voltage, & temperature variations, propagation & processing delays etc).
vi. The system shall be able to track the satellites to ensure no interruption of synchronization signal.
vii. The output signal from each port shall be programmable at site for either one hour, half hour, minute or second pulse, as per requirement.
viii. The equipment offered shall have four (04) output ports. Various combinations of output ports shall be selected by the customer, during detailed engineering, from the following:
• IRIG-B
• SNTP Port
ix. The equipment shall have a periodic time correction facility of one second periodicity.
x. Time synchronization equipment shall be suitable to operate from AC (240V) or DC (110V/220V) power supply as available at Substation.
xi. Equipment shall have real time digital display in hour, minute, second (24 hour mode)

3.8 Technical specifications of substation hardware items

3.8.1 Ethernet to Optical Media Convertor

It shall be used for connecting Ethernet output of IEM with DCU in Control Room. Broad parameters are as detailed: -

- Interface: 10/100/1000 Mbps Ethernet (RJ45)
- Optical Port: SC/ST/LC connector, as applicable
- Fiber Type: Multimode: up to 2 km
- Power Supply: 240V AC or 110/220V DC

3.8.2 Fibre Optic Cable

Suitable multi mode optical fiber cable of six cores shall be provided for connecting the IEM to the Switch for onward communication to DCU. All the cores of fiber cable are to be terminated in the LIU (Line Interface Unit) at switchyard end as well as the LIU in control room. Optical fiber in switchyard area/cable trench/cable vault shall be laid in suitable size GI pipe.

3.8.3 Power Cable:

Supply of 3 Core x 2.5 sq.mm Copper Conductor, PVC Insulated armoured Power Cable, 1100 V grade, conforming to IS 7098 (Part-1) is Bidder’s scope to meet the auxiliary power requirement of various items / components.

3.8.4 Optical Fiber LIU (Light Interface Unit) - 1U Rack Mounted

The Optical Fiber Light Interface Unit (LIU) shall be a 19-inch, 1U rack-mountable unit designed for termination, management, protection, and interconnection of optical fiber cables. The LIU shall support SM/MM optical fibers, provide adequate splice management facilities, and be supplied complete with adapter panels, splice trays, pigtails, patch cords, cable management accessories, and labeling arrangements.

Sl. No.	Description of the Features	Minimum Quantity of the Features
1	Type	19" Rack Mount Fiber Optic LIU, Fixed 1U type suitable for termination, interconnection, cross-connection, splicing and management of optical fiber cables.
2	Mounting	Rack mountable, slim 1U height design suitable for standard 19-inch rack.
3	Construction	Cold rolled steel body with aluminium front and top cover with powder coating finish.
4	Application	Suitable for optical cable termination, bare fiber splicing & protection, pigtail storage and fiber management.
5	Fiber Management	Shall support both fiber splicing and termination in a single unit.
6	Adapter Capacity	Shall support adapter panels for minimum 12 suitable ports
7	Adapter Panel Arrangement	Preassembled shelves in multiple configurations with snap-in locker design for easy replacement of adapter panels.
8	Accessibility	Removable front and top cover for easy access during installation and maintenance.
9	Cable Entry	Removable rubber grommets for cable entry and dust protection.
10	Splice Tray	ABS splice tray suitable for fiber splicing and protection shall be provided.
11	Adapter Support	Shall support SC, LC, ST and FC type adapters/connectors.
12	Port Capacity	12 Port LIU as per site requirement.
13	Fiber Type Support	Suitable for multi-Mode optical fiber applications.
14	Cable Retention	Suitable cable anchoring and strain relief arrangement shall be provided.
15	Loaded Configuration	LIU shall be supplied complete with adapters, pigtails, splice trays and all termination accessories required for commissioning.
16	Compliance	Suitable for LAN, SCADA, SAS, RTU, ICCP, AMR/Data Centre/Control Room applications and utility communication network applications.

3.8.5 CAT-6 Copper LAN Cable

The LAN cable shall be CAT-6 armoured Shielded Foiled Twisted Pair (SFTP) cable suitable for high-speed Ethernet communication in AMR, networking, and data communication applications. The cable shall support Gigabit Ethernet and provide immunity against electromagnetic interference (EMI) in substation and industrial environments.

Chapter 4 — Automatic Meter Reading (AMR) System

4.1 Intent of the AMR System

AMR system is the bridge between IEMs at Substations and the data processor system (MDP) at RLDC .The intent of AMR system proposed in this document is collection of meter load survey data at a user configurable rate (5min) and 1 minute instantaneous MW power flow data from each meter through DCU to AMR control centre for further sharing with RLDC for validation, processing and generation of customized reports by MDP system and sharing of 1 min Instantaneous MW power flow data to SLDCs for viewing purpose.

4.2 Network Architecture and End-to-End Data Flow

The meter data communication architecture comprises the Interface Energy Meters (IEMs) connected through Ethernet interface to industrial Ethernet-to-Optical Media Converters at the field /switchyard/kiosk level which aggregate and transmit metering data to the substation LAN distribution network. The data is then forwarded to the Data Concentrator Unit (DCU) through Ethernet Switch. From the DCU, the data passes through the existing local firewall and the station SDH/Fibre Optic Terminal Equipment (FOTE) before being transmitted over the ISTS Optical Fibre Network to the RLDC/RPC AMR Control Centre. At the receiving end, the communication is terminated through corresponding SDH/FOTE and secured via the AMR Control Centre firewall before being delivered to the AMR Application Server and AMR Database, with GPS-based time synchronization support.

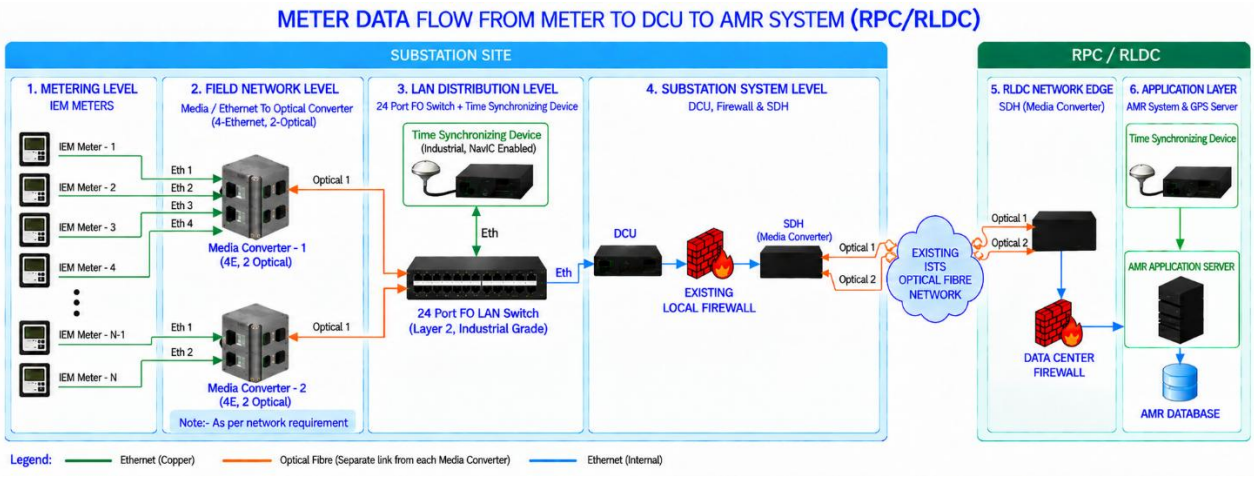


Figure 4.2 — AMR network architecture and end-to-end data flow

4.3 Scope of Work

This section provides detailed scope of work included in the bidder's scope, and also the facilities to be provided by station owner/employer.

4.3.1 Included in Contractor Scope

The scope of work in complete conformity with subsequent sections of the specification shall include site survey, planning, design, engineering, manufacturing/integration, testing, supply, transportation & insurance, delivery at site, storage, installation, commissioning, demonstration for acceptance, training and documentation of AMR system, support and maintenance including, but not limited to, the followings:

a. Provide a working system that meets or exceeds the functional and performance requirements of this specification.

b. Design Document for complete AMR System including software specifications and compliance documents with respect to Cyber Security.

c. All hardware including Application Servers, Database Servers and HMI, DCU, LAN Switches etc.

d. All cabling, wiring, terminations and interconnections of the equipment at AMR control center as well as at substation level.

e. Database development, Displays and Reports.

f. Archival and retrieval of data through Standard database management solutions

g. All firmware updates, license updates & patch updates should be in bidders scope. Any new application will go through required patch updates periodically.

h. The complete system shall be in line with established cyber security standards.

i. Training of Owner/Employer personnel.

j. Engineering and technical assistance during the guarantee and AMC period

4.4 Components of the AMR System

a. Data Concentrator Unit at substation level (as detailed in Section 3), with associated communication accessories up to the FOTE/SDH and connection to the local computer.

b. AMR system server (application + database) at the AMR Control Centre (RLDC/RPC), including its connection with the existing FOTE/SDH at the RLDC over the existing ISTS communication system

c. AMR web server, positioned in a firewall/DMZ-protected segment, hosting the RLDC data-sharing application, the SLDC 1-minute MW viewer, and the CTUIL central data-sharing interface (Section 5.1.3-5.1.4).

d. Network security and WAN equipment — firewall(s) and router(s) — supporting the SLDC and CTUIL links, as detailed in Section 5.10.

4.5 AMR Software

AMR System provided at AMR Control Centre (RLDC/RPC) will manage all functionalities of collection of load survey data along with 1 min instantaneous MW power flow data through DCUs, conversion of data to .npc format for further use by MDP system and synchronization of IEMs through DCU.

4.5 Basic Functions of the AMR System

AMR system shall support the following functions:

a. Task scheduler function for 5 min load survey data acquisition at desired interval & 1 min instantaneous MW power flow data acquisition in real time
b. Functionality for re-polling of missing data if any.
c. Raw data to [.npc] conversion.
d. Web application to share [.npc] files to RLDC.
e. Web application for viewing of 1min MW data by SLDCs.
f. 15 days storage of Raw/Binary data of 5 min load survey data at AMR control centre.

g. Monitoring of connectivity of IEMs, its time drift & Time synchronization.
h. Live system dashboard of AMR
i. DCU Live status Report

The detailed technical requirements for various functions of AMR system are described in subsequent sections. The Bidders are required to offer their standard products that meets or exceeds the specification requirements.

4.6 Functional Requirements

Main functionality of AMR system is to acquire data from different meters installed at Interface points. AMR system shall perform at least the following functions:

i. Communication with DCUs for polling of IEM data

AMR system shall communicate with DCUs mainly using ISTS Communication network. AMR system shall ensure data integrity checks, for example, checksum, time check etc. AMR system shall have polling feature to run the data downloading software at a pre-designated date and time repeatedly or by manually selecting meter. A detailed activity log shall also be available for each downloading operation.

ii. Task scheduler application

AMR system shall poll DCUs to fetch 5min load survey data and 1 min instantaneous MW power flow data from each meter automatically through task scheduler functionality at a user defined interval. It shall fetch meter data from all metering points and process the same in its server in user defined formats (text, csv, xls etc.) in a user defined file name (file name format must be dd-mm-yy substation name-utility name-meter serial no). There should be provision to select multiple meter data file based on filename and convert all selected files. The system shall display meter data (for individual meter or Station wise or Utility wise) on PC's screen in text format, with forward/backward rolling.

AMR system shall automatically retry for missed data; the number of retry attempts and the time interval between each attempts shall be configurable (max 3 attempts with configurable time gap between each attempt). After maximum attempts, the system shall generate event and alarm showing details of missing data both at Substation PC as well as in AMR server at RLDC. An automatic mail shall be generated by the system for uploading missing data through Web application.

iii. Uploading missing data through Web application

AMR system shall include a web-based application for utilities/stations to manually upload the missing data in case of AMR communication system failure due to any reasons. The following shall be taken care of in this regard:

- The web application link shall be made accessible to all stations through website.
- Only encrypted data shall be uploaded
- Each station shall be given User name and Password for login the web application.
- Browser shall have the list of all Utilities and its station names.
- Each station shall upload the encrypted data by selecting their Utility name and Station name.
- Web Application shall generate the confirmation message to the station on successful uploading of data.

- Web application shall generate the popup message at AMR system with Utility name and Station name on receipt of data and the same shall be recorded as alarm/event in AMR system.
- All the encrypted data received at AMR system via web application shall be stored in predefined path.
- AMR system shall have the provision to store the data in the database for the further processing.

Uploading meter data files manually to the AMR system by an authenticated user shall also be supported and shall be done by the operator within stipulated time to achieve availability of 5 min load survey data at AMR control centre.

iv. Collection of status/alarm data from DCUs

AMR software shall have feature to monitor each DCU for its status, parameters and any alarm, events. The status data shall be collected periodically or on demand at any time from all or selected DCUs. Upon failure of communication of DCU with AMR centre, alarm/event shall be generated by AMR system and an automatic mail shall be sent to respective stations. AMR operating personal shall co-ordinate the same with concerned person \ location as well.

v. Integration/configuration of DCUs & IEMs from remote

AMR software shall have feature for remote integration of New IEMs and DCUs without any interruption to existing process. It shall also have the functionality to configuration of selected or batch of DCUs & IEMs.

It shall be able to configure below mentioned parameters of DCU individually or in batch mode.

- Configuration of DCU for integration of New IEMs.
- Modification of database in case of replacement of IEM.
- Configuration of scheduler time for collection of energy data/Status/Alarm etc.
- Changes in meter protocol driver

It shall also be able to configure some meter parameters through DCU such as Time Block, setting reactive power band as per the changes suggested by appropriate commission in future.

Only admin user shall have the rights to configure DCU/IEM parameters from AMR software.

vi. Time synchronization of DCUs/IEMs

The AMR system shall maintain time synchronization across all devices to ensure accuracy of data. The AMR system shall check and send time synchronization to all meters once in a day, which shall be user configurable and can be modified by admin user as per the future requirement.

vii. Storage of Raw/Binary data in AMR system Database

AMR system shall support storage of 5min load survey raw meter data and alarms & events for maximum 15 days

viii. Data sharing with RLDCs, SLDCs & CTUIL

Three type of web browser application shall be designed for data sharing purpose to RLDC and SLDC.

- **For RLDC**

AMR system shall convert 5 min raw meter data in .npc format and share the same with MDP system in [.npc] format through reliable communications (i.e. Secure LAN port & OFC/LAN cable) or secure web browser through authenticated login on Web Portal. Provision should be made available for downloading meter data in suitable batches/state wise/location wise/meter wise.

- **For SLDC**

AMR system shall also provide access to SLDCs to view 1 min instantaneous MW power flow data through secure web browser for viewing purpose. The application shall be designed to sum-up the 1 min instantaneous MW power flow data for the pre-defined meters for each SLDC. This application shall have the provision for addition/ deletion the meters as per SLDC requirement. Implementing agency shall collect the details of ISTS meters from each SLDC during detailed engineering for this purpose.

- **For CTUIL**

AMR system at each RLDC/RPC shall share a consolidated feed of asset inventory data for all the regions' ISTS interface metering with the CTUIL. This data excludes load survey data required at AMR & MDP system.

- **Centralized Consoles for all Regions:** A dedicated AMR console shall be provided at CTUIL HQ for viewing and monitoring respective Region and Cross-Border IEM/SEM details (Make Model etc)
- **Meter Asset Management Dashboard:** The dashboard shall provide region wise meter asset information including meter make, model, serial number, ownership details, installation location, commissioning date, replacement history and present operational status
- **Advanced Search & Analytics:** Users shall be able to search, sort, filter, and analyse meter information based on multiple parameters such as region wise, utility, substation, voltage level, meter make, installation date, communication media (either thru e-Mail etc) and ownership etc also for details with respect to compliance for supply/installation.
- **IEM/SEM Supply & Installation, Integration with DCU & AMR-** Detailed report.
- **AI & Trend Analysis for supplied & installed Energy Meters:** The AMR system shall be equipped with AI and analytics features for trend analysis, failure pattern identification, and predictive insights across the meter population.
- **Report Generation Facility:** The console shall support generation of standard and customized reports related to meter installation, replacement, asset status and compliance monitoring etc.

ix. Reporting functions

AMR system shall have live system dashboard & data reporting capability implemented through a separate module. Reporting module shall give report output on screen in pdf or in .xls/,csv form at user configurable format & periodicity.

Some of the required reports are as below

1 Meter Master file, Utility wise, Station wise (As and when required)

2 Meter details; Utility wise, Station wise, month wise, year wise, or as per customized period (As and when required)
3 Missing Meter Data report (after completion of each polling cycle)
4 DCU disconnection report (Daily/Weekly/Monthly)
5 Time Synchronization Report (Daily)
6 Meter Database change report (Monthly)
7 Software/Patch updation Report (As and when required)

Report formats shall be finalized during detailed engineering in association with Employer/Owner. System shall process print out of any report as per operator's instruction.

x. Monitoring and alarm generation

AMR system shall generate alarm and event log whenever "data not received" occurs for each polling cycle from one or more DCUs/IEMs. The alarm shall indicate which location/DCU/IEM has the problem.

xi. Audit trail and logging

AMR system shall have security features to prevent unauthorized access to IEMs and meter data to ensure authentication for all AMR components. The system shall have audit and logging function for each and every activities either completed successfully or failed.

The system shall provide audit trail of user and system activities that enables data changes to be tracked and reported, including changes made by the system administrator.

For editing of energy meter data, the system shall record the following information in a log and store it for a minimum of 12 months:

- User ID
- Date and Time of Change

User shall be prompted to input a reason for editing using either a standard reason code or a freeform text field. In addition to data stored in the edit log, each interval containing edited data shall be marked with a status to indicate that the data has been edited. The pre-edited value shall be stored in the database as a previous version, which can be retrieved using "as- off" date functionality.

Changes to configuration data by users shall be logged by date, time, and user ID and such logs shall be stored for a minimum of 12 months. Critical changes relating to measuring parameters (pulse multipliers, transformer ratios, etc.) and formulae change shall be stored indefinitely as a previous version. The database for these is to be maintained in AMR system.

It should have provision of full data for system audit ability such as version controls and data retrieval according to the date and time. The functionalities other than specified here to meet the intent of AMR shall also be considered by the contractor as part of AMR without any extra cost.

xii Multi-Vendor Interoperability

Because IEMs, DCUs and the AMR system may, over the life of the ISTS metering scheme, be sourced from different manufacturers at different times, the entire solution shall be designed for multi-vendor interoperability. DCUs shall be capable of reading data from all makes of IEM supplied in conformity of this specification, using the common DLMS protocol and IS 15959

frame structures, and the AMR system shall be capable of polling and processing data from multiple DCU makes without requiring proprietary, vendor-locked extensions.

4.7 AMR System Sizing

The sizing requirement specified in this document is only for initial sizing. The delivered system shall be expandable as per future requirements up to 50%. Vendor is required to demonstrate their system's expandability in FAT (Factory Acceptance Test)

i. Population of Energy Meters

Each Regional AMR system shall be capable to receive data from 500 to 1000 DCUs and each DCU shall be capable of connecting at least 30 IEMs. Further, AMR system shall have provision to collect and handle data from 15000[$] energy meters without any significant degradation of performance.

$These are tentative numbers. Exact no. of IEMs & DCUs shall be as per concurrence of respective RPCs at the time of detailed engineering and tendering stage.

ii. Data Storage

AMR system shall support storage of raw meter data, alarms, and events for 15 days beyond which the data shall be removed from database in FIFO mode. The storage shall be calculated considering 50% space availability as spare all time with maximum Meters connected (i.e. 15000 numbers of IEMs).

4.8 Performance Requirements of AMR System

The AMR system shall receive the load survey data from all meters in the region including missing data on same day as per schedule agreed in the detailed engineering. AMR system shall poll DCUs/IEMs in batches; each batch shall consist minimum 1000 meters; and receive complete data from all concerned DCUs/meters within 1 hour including re- polling of missing data (if any).

AMR system shall continue to operate without interruption under any single point of failure condition. That means there shall be no hardware or software element whose failure renders the AMR system unavailability.

4.9 Software requirement of AMR System

AMR system shall be developed on open platform based on distributed architecture for scalability without degradation of the performance using additional hardware in future (if required).

AMR System shall meet the following general software requirements.

i. Upgradability

Operating System, application programs supplied in AMR system shall be fully upgradable by firmware upgrade or other software upgrade methods. The same shall be logged in the system.

ii. Cyber Security

Third Party security audit by CERT-in certified auditor is to be done prior to commissioning or Go Live whichever is earlier. Compliance with CERT-in standard & CEA (Cyber security in power sector) guidelines 2026 for all software modules has to be ensured by suppliers prior to handing over. Supplier/Contractor shall document and implement a Cyber Security Policy in line with

CERT-in latest guidelines (https://www.cert-in.org.in) to secure the system and the Contractor shall keep updating the Security settings as per the revised guidelines of CERT-In at time to time.

Minimum requirements to be followed by the contractor for making the entire AMR system immune to Cyber-attacks are as follow

- All the Hardware, OS and application software shall be hardened
- Network partitioning and DMZ by use of firewall as required while facilitating access for data to RLDC and SLDCs
- All default user id & password shall be changed after first time Log in.
- All log in / log out and cable plug in/plug out shall be logged in the system
- Authorization control shall allow only to use or access functions for which they have been given authorization. The access privileges for each user can only be assigned by system administrator of AMR system as the case may be.
- System and application sessions must automatically lock after 30 minutes (configurable) of inactivity.
- Record all network traffic for detecting unauthorized activity, unusual activity and attempts to defeat system security.
- Vendor must identify and list the entire network and other protocols that is used for AMR system and limit what is not required.
- All unused USB ports, Wi Fi, & Infrared driver of all servers/workstations shall be disabled at AMR control center.
- Use of encrypted communication between substation to AMR System at RLDC/RPC and between RLDC/RPC to SLDC/CTUIL.
- Blocking of unused ports in network switches/ firewalls

4.10 Documentation requirements of AMR system

Documentation of AMR system shall meet following requirements. All documents shall be supplied in hard copies as well as computer readable soft version.

i. Design Documents

Before manufacturing of the AMR system components, a design document shall be submitted. The design document must essentially (but not limited to) include following:-

- System Overview & complete network schematics
- Functional/ Flow chart diagram
- Functions/ Technical Details of major component
- System configurations & Design Documents
- Testing Procedure (Type/Routine Test ,FAT, SAT)
- Cyber Security policy as per CERT-in guideline and Compliance report to CERT-In standard & CEA (Cyber security in power sector) Guidelines 2021 and amendments thereof.

ii. User Manuals

A list and brief description of all user documents that will be provided along with the software package to be supplied during system handover. This must include the following minimum documents:

- System configuration manuals
- Technical support handbook
- User Manuals for complete AMR system including DCU
- Operation & Maintenance Manuals of AMR system including DCU.

User manual for central site location where AMR system shall be installed and where all data collection activities shall be taken up, should contains all user instructions, block diagrams, user screens etc. in order to make itself contain complete document required for operation of complete AMR system including each and every component of the metering system.

A comprehensive documentation including product manual, Installation manual, O&M manual for DCU along with video tutorials to attend minor issues shall be uploaded and made available at AMR server. The same shall be accessible from all connected substations through web application link.

Chapter 5 — Control Centre Hardware and Infrastructure

5.1 General

The Contractor shall design, supply, install, configure, test and commission all Control Centre Hardware and Infrastructure required for successful operation of the AMR System and its interface with the existing Meter Data Processing (MDP) System of RLDC.

The Control Centre Infrastructure shall comprise, but not be limited to:

- Application Servers
- Database Servers
- Communication Servers
- Web Servers
- Storage Systems
- Network Switches and Routers
- Firewalls and Cybersecurity Appliances
- Backup Systems
- Virtualization Platforms
- Operating Systems and Associated Software Licenses
- System Monitoring and Management Tools

The infrastructure shall provide a reliable, scalable, secure and high-availability platform for acquisition, storage, processing, monitoring and retrieval of metering data.

All supplied equipment shall be industrial-grade and suitable for continuous 24x7 utility-critical operation.

The Contractor shall carry out all activities associated with installation, configuration, testing, commissioning and operationalization of the AMR System Infrastructure. This shall include hardware installation, operating system installation, database configuration, network configuration, cybersecurity hardening, performance tuning, backup configuration, integration testing and operational acceptance testing. The Contractor shall additionally provide all technical documentation, architecture drawings, configuration records, inventory details, operation manuals, maintenance manuals and as-built documentation necessary for operation and maintenance of the infrastructure.

5.2 Server Hardware - Minimum Requirement

Sl. No	Description of the Features	Minimum Quantity of the features
1.	Application	----
2.	Manufacturer	----
3.	Model No.	----
4.	Specint & Specfp	As per the base runtime requirements of SPEC CPU 2017 Benchmarking Standards.
5.	Processor	Min 2x16 core, x86 64-bit fourth generation or latest processor (with compatible chipset) with 2.5 GHz or more base frequency The OEM software should be tested on the offered processor & chipset

6.	RAM	256 GB delivered, expandable up to 386 GB or Above DDR4 RDIMMs/LRDIMMs. The operating system delivered should support expansion up to 386 GB of RAM.
7.	Internal Auxiliary memory	3.84 TB usable capacity of SSD NVMe after RAID 1 disk configuration, expandable up to 8 TB, Hot-pluggable
8.		
9.	Interfaces	1. 2 x 10 Gbps FO ports 2. 3 Dedicated 1 Gbps Management port 3. 2 x 16 Gbps FC port for NAS connectivity
10.	User interface	Through KVM switch & console.
11.	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, monitoring of I/O card & system health. • Out-of-band hardware & firmware inventory • Auto configuration to auto deploy a baseline server configuration profile. • Automated hardware configuration and deployment to multiple servers
12.	Server Security	Should provide effective protection, reliable detection & rapid recovery using: - Silicon-based Hardware Root of Trust - Signed firmware updates - Secure default passwords - Configuration and firmware drift detection - Automated event logging including user activity - Secure alerting - Automatic BIOS recovery - OS recovery - System erase Should provide system lockdown feature to prevent change (or "drift") in system firmware image(s) & prevent malicious modification of server firmware
13.	Mounting	Rack mountable Server
14.	Certification and compliances	Microsoft Windows Server, Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES).
15.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for memory, CPU, SSD.
16.	Power Supply	Redundant Hot plug Power Supplies with redundant fans.
17.	Heat Load	
18.	Type of Machine	Physical

The above requirements may be considered for Automatic Meter Reading (AMR) System, Server For Reporting & Dash Boarding, Web Servers, Data Historian Server, Data Replica Server, Proxy Server, Antivirus Management Server, Identity And Patch Management Server, Intrusion

Detection System HIDS/NIDS, SIEM (Security Information and Event Management) server, Centralised Management Console.

5.3 HMI (Workstation) Hardware — Minimum Requirement

Sl. No.	Description of the Features	Minimum Quantity of the Features
1	Manufacturer	----
2	Model No.	----
3	Processor	Minimum 16-core latest generation processor (along with latest chipset), base clock speed 3.0 GHz or higher.
4	RAM	32 GB DDR4 ECC RAM, expandable up to 64 GB, minimum 2133 MHz or higher.
5	Dedicated Graphics Card	Minimum 4 GB dedicated graphics memory.
6	Internal Memory	1. 512 GB SSD (Primary Drive) 2. 512 GB SATA HDD, expandable up to 1 TB.
7	Optical Drive	DVD-RW.
8	Audio	Integrated audio with internal speaker.
9	Interfaces	Two (02) Gigabit Ethernet ports, USB ports (minimum 4 nos.), HDMI/Display Port, Universal Audio Jack.
10	User Interface	Two 23.8-inch widescreen monitors (16:9 aspect ratio), Full HD resolution (1920 × 1080), anti-glare coating, LED colour display, keyboard and optical mouse.
11	Operating System	Pre-installed OEM licensed Microsoft Windows Professional latest 64-bit or latest equivalent operating system installed on primary SSD.
12	Certifications and Rating	Energy Star 6.1 compliant or higher.
13	OS Certifications	Certified for Microsoft Windows and Linux operating systems.
14	Security	TPM2.0
15	Mounting	Desktop mounting
16	AC Power Supply (in Watts)	----
17	Heat Load	----

5.4 Remote Console (All-in-One)

Sl. No.	Description of the Features	Minimum Quantity of the Features
1	Manufacturer	----
2	Model No.	----
3	Processor	Minimum 8-core latest generation processor (along with latest chipset), **Clock Speed 2.4 GHz or higher** (base frequency).
4	RAM	16 GB RAM supplied, expandable up to 64 GB DDR4 Non-ECC/ECC RAM, minimum 2133 MHz or higher.
5	Dedicated Graphics Card	Minimum 4 GB dedicated graphics memory.

6	Internal Auxiliary Memory	512 GB SSD.
7	Optical Drive	DVD-RW.
8	Audio	Integrated audio with internal speaker.
9	Interfaces	One (01) Gigabit Ethernet port, USB ports (minimum 4 nos.), HDMI Port/Display Port, Universal Audio Jack.
10	User Interface	23.8" widescreen display (16:9 aspect ratio) or larger, Full HD resolution (1920 × 1080), anti-glare coating, wide viewing angle WLED monitor, keyboard and optical mouse.
11	Operating System	Preinstalled OEM licensed Microsoft Windows Professional latest 64-bit or latest equivalent operating system installed on primary SSD.
12	Certifications and Rating	Energy Star 6.1 compliant or equivalent.
13	OS Certifications	Microsoft Windows and Linux OS certified.
14	Mounting	Desktop mounting.
15	Security	TPM 2.0 support.
16	AC Power Supply (in Watts)	OEM supplied power supply suitable for offered configuration.
17	Heat Load	-----

5.5 LAN Switch — Minimum Requirement

a. Compliant with ISO 8802/IEEE 802 series standards; rack-mountable, 1U form factor.

b. Hot-swappable, field-replaceable internal redundant power supply and fan, from day one.

c. Support Layer-3 routing for both IPv4 and IPv6 (static route) and VLAN.
d. Shall support both IPv4 and IPv6 simultaneously.
e. 24 Port (Minimum 4x10 Gbps Fibre Optic Ports And 8x1 Gbps Ethernet Ports) (exact port count per network architecture; multiple switches supplied as required).

f. 1 x USB console port, 1 x out-of-band management port, 1 x serial console port.

g. Flash memory ≥128 MB, DRAM ≥512 MB; Cat-6 or higher cabling.

h. Hardware-based ACL support (VLAN, port, MAC, IP-based); SNMPv1/v2c/v3 support; manageable via SSHv2/SSL/SNMPv3.

i. Full IPv6 compliance without additional hardware/software.

5.6 Network Attached Storage (NAS)

The NAS shall provide centralized, reliable, and secure storage for IEM/AMR applications, logs, reports, configuration files, backups, and archival data. The solution shall support continuous operation in a control center environment.

Sl. No	Description of the Features	Minimum Quantity of the features
1.	Capacity	Minimum usable capacity of 10TB
2.	Spare HDD	2 Nos.

3.	Processor	Min 2x6 core, x86 64-bit latest processor (with latest chipset)
4.	RAM	64 GB delivered or above DDR4
5	Expandability	Min 50% expandable including slots with storage enclosure
	RAID level	6
5.	Hard Drives speed	enterprise-class SSDs
6.	Hot swappable Hard Drives	Yes
7.	Dual Power Supply	Yes
8.	Heat Load	
9.	Interface Ports	Minimum 4*10G (either Base T ports or FO ports)

NOTE: Storage capacity of SAN and NAS doesn't include the SIEM logs storage capacity (as p er TS requirement). Log storage capacity of SIEM varies from OEM to OEM as per compression ratio, hence, storage space for SIEM log shall be considered additionally over and above the spe cified SAN storage capacity for the control centre without any additional cost to Owner.

5.7 Server Rack Panel 44U

The rack shall be suitable for housing servers, storage systems, network equipment, and associated accessories in a data center or control center environment. The rack shall be supplied complete with an IP-based KVM switch, rack-mounted LCD monitor, keyboard, and all mounting accessories

1. Rack Specifications

- Standard **19-inch, 44U floor-standing rack cabinet**.
- Dimensions suitable for accommodating enterprise servers and networking equipment.
- Front toughened glass door and perforated rear door for ventilation.
- Lockable front and rear doors with side panels.
- Adjustable mounting rails.
- Static load capacity: Minimum **1000 kg**.
- Cable entry provision from top and bottom.
- Powder-coated steel construction.

2. Cooling & Ventilation

- Adequate ventilation through perforated doors.
- Minimum 4 Nos. high-speed cooling fans with power distribution.
- Fan failure indication preferred.

3 Power Distribution

- Rack-mounted Power Distribution Units (PDUs).
- Minimum 2 Nos. 8/12-port PDUs with surge protection.
- Input Supply: 230V AC, 50Hz.

4 IP-Based KVM Switch

- Enterprise-grade IP-enabled KVM switch.
- Minimum 16 server ports, expandable if required.
- Remote BIOS-level access through LAN/WAN.
- Support for virtual media and remote reboot functionality.
- User authentication and role-based access control.
- Support for IPv4/IPv6.
- SNMP and web-based management interface.

5. Rack-Mounted LCD Console

- 1U or equivalent rack-mounted LCD monitor with integrated keyboard and touchpad.
- Monitor size: Minimum 17-inch LCD TFT.
- Resolution: Minimum 1280 × 1024.
- Slide-out rail-mounted design.
- Compatible with installed KVM switch.

6. Accessories

- Cable managers (horizontal and vertical).
- Blank panels for unused rack spaces.
- Cage nuts, mounting screws, grounding kit, and power cords.
- Proper rack earthing arrangement.

7. Environmental Conditions

- Operating Temperature: 0°C to 40°C or better.
- Relative Humidity: 10% to 90% non-condensing.

5.8 Data Diode & Other Accessories

Contractor to install data diode at control center for data ingestion from AMR server. Further details shall be provided during detailed engineering.

Specification of Data Diodes are as follows:

Sl. No.	Category	Specification
1	**Physical Requirements**	
A	Dimensions	
B	Power Supply	100–240V AC, 50 Hz
C	Operating Temperature	5°C to 50°C (non-condensing)
D	Storage Temperature	-10°C to 60°C (non-condensing)
E	Humidity	10% to 90% (non-condensing)
F	Physical Interfaces	Ethernet / Gigabit Optical
2	**Network Interfaces**	
A	Ethernet	10/100 Mbps – At least 1 input and 1 output (For Proxy)
B	Fiber Optic	10 Base-SX – At least 1 input and 1 output (For Diode)
3	**Technical Requirements**	
A	Supported Protocols	• Transport: TCP/IP, UDP • File Transfer: SFTP • Messaging: SMTP, Syslog, MQTT • Industrial/OT: OPC UA, Modbus • Web/API: HTTPS • Monitoring: SNMP, NTP
B	Proxy Servers	Inbuilt proxy servers in data diode hardware box or separate hardware for proxy servers. Proxy servers shall be provided with following protocols: TCP/IP, UDP, SFTP, SMTP, SYSLOG (all at a time).
C	Visibility	The hardware of data diode should be able to break protocol and should form non-routable connection.
D	Data Transfer Rate	5 Mbps or higher

F	Low Latency	Data Diode shall be designed to minimize latency in data transmission, ensuring timely data transfer. Latency < 1 ms
4	**Compliance Requirements**	
A	Security Standards	Common Criteria (EAL4+) or higher
5	**General Requirements**	
A	One-Way Data Transfer	Enforced by hardware design (not software)
B	Electrical Isolation	Complete electrical isolation to prevent reverse data flow and signal leakage. Data transmission through optical communication.
C	Error Detection and Correction Algorithms	Data Diode solution shall protect the identified network from cyber threats while maintaining one-way connectivity. The configuration should be encrypted, and any change should be governed using a hardware secure crypto key.
D	Protection from Cyber Threats	Data Diode solution shall protect the identified network from cyber threats while maintaining one-way connectivity. Shall not pass on the IP address/MAC address of the internal or external device.
E	Monitoring	Integrated tools for monitoring data transfer status and performance.
F	Logging	Logging capabilities for auditing and compliance. Log storage for at least 10 days.
G	Management Interface	Web-based and command-line interface
H	Redundancy	Redundant power supplies for high availability
I	Power Cables	As Required
J	LAN Cables	As Required
K	Software	Data Diode solution shall be supplied with requisite software tools for realization of one-way data transfer solution through hardware data diode.
L	Blocking Unwanted Functionality	Data Diode shall have provision for blocking unwanted/unused functionalities offered by the solution.
M	SNTP	Data Diode solution shall support Network Time Protocol for time synchronization.
N	Other Accessories	Any other accessories required shall be provided/supplied.
6	**Central Management / Administration**	
A	Remote Control of Data Diode (through Proxy Servers)	Data Diode shall support remote access for central management of the device.

5.9 Processor Terminal -Laptop

The Processor Terminal Laptop shall be used for configuration, monitoring, testing, diagnostics, data collection, report generation, troubleshooting, and maintenance of the Automated Meter Reading (AMR) system, communication equipment, and associated applications.

Sl. No.	Description of the Features	Minimum Quantity of the Features
1	Manufacturer	----
2	Model No.	----

3	Processor	Minimum 4 Core latest generation processor (along with latest chipset) with **3.0 GHz clock speed or higher** (base frequency).
4	RAM	16 GB DDR4 RAM, minimum 2133 MHz or higher.
5	Dedicated Graphics Card	Minimum 4 GB dedicated graphics memory.
6	Internal Auxiliary Memory	512 GB SSD.
7	Mouse	Wireless Mouse.
8	Keyboard	English Keyboard with Backlight.
9	Wi-Fi Wireless LAN Adapter	**Dual Band Wireless + Bluetooth 4.0** or higher.
10	Interfaces	One (01) Gigabit Ethernet Port, minimum two (02) USB Ports, HDMI Port/Display Port, Universal Audio Jack.
11	Screen	15-inch or larger Full HD Display (1920 × 1080) with Full HD Webcam.
12	Operating System	Pre-installed OEM Licensed Microsoft Windows Professional latest 64-bit or latest equivalent operating system installed on primary SSD.
13	AC Power Supply (in Watts)	OEM supplied AC Adapter suitable for offered configuration.

5.10 Wan Routers At Server Location End

Routers are the device which is used to send/receive signals coming from node directly to access points. It shall use dynamic message routing. It shall have data security and error checking algorithms to achieve integrity & reliability. The installation of routers shall be suitable for clamp mounting on poles or DIN-rail mounting on distribution panels. Any other suitable mounting arrangement required for access point installation shall also be provided. Access point shall be used for collection of data coming from various nodes and transmission of the same to AMR System in Control Centre.

Necessary control should be applied on the router to stop unwanted traffic and attacks at the perimeter itself. In the secure configuration of a router, the following strategies should be considered.

- Deploy proper access management and avoid remote administration.
- Enable password.
- Change default SNMP community string.
- ACLs (Access Control Lists) should include
- Apply egress/ingress filter
- Filter all RFC 1918, 3330 address space and special/reserved address
- Permit the required services for the required IP addresses only Deny everything else.
- Turn on logging to a central syslog server.

Sr. No.	Description of the Features	Minimum Requirement of Features
1	Manufacturer	----
2	Model No.	----
3	Functions	High performance Routing for data exchange between data centres, remote WorkStation, DCU
4	Routing Capability	Layer-2 & Layer-3 routing & Dynamic discovery of routing
5	Processing capacity	Minimum 2 Mbps
6	Features to support	QoS, MPLS, Security, Broadband, Multiservice, Voice, IP to IP Gateway
7	Routing protocols	IS-IS, OSPF, BGP, ARP, IPCP, IP forwarding, VLAN & MPLS etc.
8	Network protocols	TCP/IP, IPv6, IPv4, OSI, Telnet, UDP, DHCP
9	Network management	Using SNMP Protocol
10	Inbuilt security features	**a.** Data encryption supported DES (56 bits), 3DES (168 bits) and hashing algorithms like MD5 and SHA-1. **b.** Filtering of packets based on Source address, Destination address, Protocol type, User, Port number, URL. **c.** Filtering of protocols such as FTP, SMTP, HTTP, SNMP, UDP, ICMP, RPC, DNS, DHCP, ARP. **d.** Minimum 100 IPSec VPN tunnels support. **e.** Detailed system logging.
11	Speed configurability at each port	All ports shall be configurable from 64 kbps to 2 Mbps
12	Interface ports	Minimum 4x10 Gbps Fibre Optic ports, 8x1 Gbps Ethernet Ports
13	Mounting	Rack mountable

5.11 Internal/External Firewall with IDPS For Server Location

All firewalls shall be hardware box firewall as per the requirements mentioned in Below table. Vendor has to keep all license updated throughout the contract period and provide the license validity till the completion of contract including AMC (including extension if any).

All the data exchange from outside the control centre shall be routed through Firewall only. The contractor shall provide a Network-based intrusion detection and prevention system coupled with the Firewall solutions to detect and prevent intrusion, worm, virus etc. Its main functions also include protecting the network from threats, such as denial of service (DoS) and unauthorized usage. It monitors the network for malicious activity or suspicious traffic by analyzing the protocol activity. This, in turn, makes the network intelligent and quickly discerns good traffic from bad traffic. Definition updates for virus, signatures, software patches etc. shall be done up to AMC period. External Firewall (DMZ) shall support Multi-Factor Authentication (MFA) functionality also which shall be used for VPN and other purposes. MFA shall generate one-time password (OTP) and shall be available to the users via SMS, E-mail, through mobile application or dedicated token-based devices.

As per the proposed BOQ all the external, internal firewalls should be properly configured to segregate networks into different segments. Firewall shall have the features of Next Generation Firewall to secure the system more effectively. OEM of the firewall shall use global footprint of

security deployment for more comprehensive network protection. The firewalls should have the following features including requirements mentioned in respective DRS.

- Application awareness and control: Firewall shall have the feature of identifying applications in the network and enforcing security policy at the application level itself.
- Identity awareness: Firewall shall have the feature of integrating with applications like active directory and enable firewall rules to individual users or user groups.
- Firewall shall be able to receive threat intelligence feeds from time to time to detect threats and prevent attacks.
- Firewall shall provide easy integration with other devices like SIEM etc.
- Firewall solution shall support minimum 10000 IPS, minimum 2000 applications signatures and risk-based control that can invoke tailored IPS threat detection policy through optimized security effectiveness. These performance numbers must be available on Firewall Dashboard/GUI.
- Firewall device shall have the Geo-location based IPv4 & IPv6 database. So that Geo-location-based traffic filtering shall be done in the device. The device shall regularly update their Geo-Location base lPv4 & lPv6 database from the Global repository.
- Next Generation Fire Wall shall support on-premises sandboxing (Anti-APT, to be procured separately) feature to protect against zero-day attack if required in future.
- CVE (Common Vulnerabilities and Exposures) of Firewall OS shall be available /disclosed publicly in website.
- Firewall solution shall be purpose-built appliance and should not have wireless access and Bluetooth component within its hardware and software to facilitate direct connectivity (wirelessly) with firewall.
- Firewall solution shall provide IPv4 and IPv6 dual stack support from day one and
- The proposed Firewall / Firewall Operating System shall be tested and certified for **EAL4**+/ NDPP (Network Device Protection Profile)/NDcPP (Network Device Collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, DEIT, Govt. of India.
- Detection and inspection of encrypted traffic; intrusion detection and prevention user controlled updates; detection, inspection and filtering based on signature and behavioral anomalies shall be included in intrusion detection and prevention feature.
- Firewall shall support both online/offline signature updates.
- The **external** and **internal firewalls** shall be of different makes

The following strategies shall be followed for secure configuration of firewalls.

- Clean-up rule.
- Place a ‘Deny Any-Any’ rule at the end of the rule base.
- Never create an ‘Allow any-any’ rule.
- Allow rules should be created only for required services.

This will result in all traffic being disallowed, unless specifically allowed.

- Lockdown/stealth rule
- All traffic destined for the firewall itself should be disallowed.

- Anti-spoofing rule.
- Place anti-spoofing rule as per RFC 1918 and 2827.
- Enable DoS/DDoS features on Firewall
- Enable application-level filtering of firewall
- It should show policy traffic trend over the day with host and destination addresses by selecting on each policy
- **Geofencing shall be enabled in all the firewalls and security devices.**

External Network Firewall with NIPS

Sl. No.	Description of the Features	Minimum Quantity of the Features
1	Manufacturer	----
2	Model No	----
3	**General** a. The appliance-based security platform should provide Firewall, AVC, Anti-malware, Anti-Bot, Anti-Spyware, URL and IPS functionality in a single appliance from day one. b. Proposed appliance shall have minimum 200 GB SSD drive; however, size must be considered to meet other requirement specified under the specification. c. Multicore CPU architecture with a hardened 64-bit operating system to support higher memory with minimum 6 physical CPU cores on the device and minimum 16 GB RAM on device or higher. d. Firewall should have integrated redundant hot-swappable power supply. e. Firewall should have redundant fan. f. Local/Centralized logs storage (traffic/audit/system) for at least 180 days. g. Common Criterial Certification for minimum EAL4+ level	
4	**Sizing Parameters** **a.** Should have Minimum NG Threat prevention throughput in real world/production environment (by vendor third-party test report) as specified in subsequent clauses. enabling and measured with Application-ID/AVC, NGIPS, Anti-Virus, Anti-Spyware, Anti Malware, Anti Bot, Zero-day attacks and logging security threat prevention features enabled – 6 Gbps real world/production environment/Application Mix. b. Firewall should support at least 3000 new connections per second or more and shall support at-least 1 Million concurrent session/connection with all application control enabled. c. No of VLANs – 100 d. Minimum IPSec VPN peers – 200 e. Firewall should have at least 1.5 Gbps of VPN throughput.	
5	**NG Firewall Features:** a. Should support manual NAT and Auto-NAT, Static NAT, Dynamic NAT, Dynamic PAT. b. The firewall should have the capability of identifying, network hosts, network traffic from both virtual and physical machines and their activities. c. Should be capable of detecting and blocking IPv4 and IPv6 attacks including capabilities like DNS sinkhole/equivalent. d. Solution should support capability to detect threats emerging from inside the network.	

	e. The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor. f. The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.). g. The proposed firewall shall perform content-based signature matching beyond the traditional hash base signatures. h. The proposed firewall shall be able restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports. i. The proposed firewall shall be able to protect the user from the malicious content upload or download by application/protocol by enforcing the total threat protection for known and unknown malicious content such as virus, malware or a bad URL. j. Support NAT, PAT & Policy based NAT/PAT, Mapped IP (MIP), Virtual IP(VIP) & MIP/VIP grouping. k. IPSec and SSL VPN Tunneling. IPsec VPN Authenticaion Mechanism: Pre-shared keys, X.509 certificates and support for Perfect Forward Secrecy (PFS) in IPsec l. Support simultaneous operation with both IPv4 and IPv6 traffic m. URL filtering and behaviour analysis to detect and deal with threats such as malware, ransomware and SQL injection n. Denial of Service (DoS) & Distributed Denial of Service (DDoS) prevention o. Definition updates for virus/signatures/engine upgrades/software patches for the complete AMC period. p. the traffic shall be decrypted before NIPS inspection q. firewall shall support both online/offline signature updates r. Support for VDOMs	
6	Data Encryption Support	DES, 3DES, AES 128-bit, 256-bit
7	Support Active-Active Mode	Yes
8	Tunneling Functionality	NAT66 (IPv6-to-IPv6), NAT64 (IPv6-to-IPv4) & NAT46 (IPv4-to-IPv6) / IPv4 over IPv6.
9	IP Address Assignment Features	PPPoE, DHCP
10	IPv6 Features	Syn Cookie, Syn-proxy DoS attack detection, SIP, ALG's, BGP4, DHCPv6 Relay, IPv4 to IPv6 translations & Encapsulations.
11	System Management and Configuration	Using web GUI/client based (without any limitation in number of clients), Command Line Interface (console/telnet/SSH).
12	Supporting Protocols	FTP, **SFTP**, SMTP, HTTP, HTTPS, SNMP, UDP, ICMP, RPC, DNS, DHCP, ARP, TCP, POP3, IGMP, PIM.
13	Authentication Protocols	RADIUS, LDAP methods
14	Routing Protocols	Static, RIP, OSPF, OSPFv3 and BGP, BGPv6.
15	Content Filtering	JAVA & ActiveX blocking
16	**Proposed FW shall also support** a. DoS & DDoS prevention b. TCP reassemble for fragmented packet protection	

	c. Brute Force attack mitigation d. SYN cookie protection e. Zone/Interface based IP spoofing f. Malformed packet protection g. Stateful packet inspection h. Detail logging and packet capture	
17	Filtering	Filtering of packets based on Source address, destination address, protocol type, user, port number, URL (**including URL blocking**).
18	Threat Intelligence	The Appliance OEM must have its own threat intelligence analysis center and should also use the global footprint of security deployments for more comprehensive network protection.
19	Geo-Location Based Policy	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location.
20	Threat Quarantine Capability	Solution should support the capability to quarantine/blocking endpoint traffic by integrating with threat feeds from other security solution like Network Admission Control, if provisioning of additional licensing is required same may be considered.
21	Interface Requirement	a. Minimum number of 1 Gbps LAN ports: **8** b. Minimum number of 10 Gbps FO ports: **8** c. Separate HA port All the SFP+ ports should have compatible transceivers (short range transceiver) along-with required FO cables.
22	VPN & Remote User Access	The proposed solution should have VPN license for **20 Users** for firewall placed in DMZ only. The proposed Firewall should be able to perform URL filtering capability for remote user's as well, either using VPN or any similar technology (user accessing SCADA infrastructure through VPN shall bind with SCADA security policy and not be able to use restricted activity during VPN connection). If any extra hardware/software is needed to achieve this, same shall be provided from day 1 without any additional cost. Multi-factor/OTP Authentication for 20 users shall be provided from Day-1. The proposed solution based on appliance/VM must be scalable and should support integration with Active Directory/LDAP. It must provide capability to users to resolve their own password issues, registration etc. to ensure improved user satisfaction.
23	Multifactor Authentication	Email for **20 Users** (through FW placed in DMZ or separate application).
24	Operational Readiness	All features in the firewall should be functional/operational within 5 minutes of Power ON.

25	Policy Deployment Time	Any new policy/policies should be applied in the firewall in not more than 5 minutes. The time shall be measured from the pushing of the policy from management console to the policy becoming effective.
27	Power Supply (in Watts)	
28	Heat Load	
	End-of-Life (EOL) and End-of-Support (EOS) for 7 years as per TS	
	Support for Patches for 7 years as per TS	

Note: In case of any license is required, same shall be provided by the contractor during the contract period without any extra cost

Internal Network Firewall with NIPS

Sl. No.	**Description of the Features**	**Minimum Quantity of the Features**
1	Manufacturer	----
2	Model No	----
3	General	**a.** The appliance-based security platform should provide Firewall, AVC and IPS functionality in a single appliance from day one. **b.** Proposed appliance shall have minimum 200 GB SSD drive; however size must be considered to meet other requirement specified under the specification. **c.** Multicore CPU architecture with a hardened 64-bit operating system to support higher memory with minimum 6 physical CPU cores on device and minimum 16 GB RAM on device or higher. **d.** Firewall should have integrated redundant hot-swappable power supply **e. Firewall should have redundant fan.** f. Local/Centralized logs storage (traffic/audit/system) for at least 180 days. g. Common Criterial Certification for minimum EAL4+ level
4	Sizing Parameters	a. Should have Minimum NG Threat Prevention Throughput in real-world/production environment (by enabling and measured with Application-ID/AVC, NIPS, Anti-Virus, Anti-Spyware, Anti Malware, Anti-Bot, Zero-day attacks and logging security threat prevention features enabled) of **6 Gbps real-world/production environment/Application Mix**. b. Firewall should support at least 3000 new connections per second or more and shall support at least 1 Million session/connection with all application control enabled. c. No. of VLANs – 100. d. Minimum IPSec VPN peers – 1000. e. **Firewall should have at least 1.5 Gbps of VPN throughput.**

5	NG Firewall Features	a. Should support manual NAT and Auto-NAT, Static NAT, Dynamic NAT, Dynamic PAT. b. Should be capable of detecting and blocking IPv4 and IPv6 attacks including capabilities like DNS sinkhole/equivalent. c. Solution should support capability to detect threats emerging from inside the network d. The solution must provide IP reputation feed that comprises several regularly updated collections of poor reputation IP addresses determined by the proposed security vendor. e. The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.). f. The proposed firewall shall perform content-based signature matching beyond the traditional hash base signatures. g. The proposed firewall shall be able to restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports. h. The proposed firewall shall be able to protect the user from malicious content upload or download by application/protocol by enforcing the total threat protection for known and unknown malicious content such as virus, malware or a bad URL. i. Support NAT, PAT & Policy-based NAT/PAT, Mapped IP (MIP), Virtual IP (VIP) & MIP/VIP grouping. j. the traffic shall be decrypted before NIPS inspection k. firewall shall support both online/offline signature updates l. Support simultaneous operation with both IPv4 and IPv6 traffic m. Denial of Service (DoS) & Distributed Denial of Service (DDoS) prevention n. Definition updates for virus/signatures/engine upgrades/software patches for the complete AMC period
7	Data Encryption Support	DES, 3DES, AES 128-bit, 256-bit
8	Tunneling Functionality	NAT66 (IPv6-to-IPv6), NAT64 (IPv6-to-IPv4) & NAT46 (IPv4-to-IPv6) / IPv4 over IPv6.
9	Support Active-Active Mode	Yes
9	IP Address Assignment Features	PPPoE, DHCP
10	IPv6 Features	Syn Cookie, Syn-proxy DoS attack detection, SIP, ALG's, BGP4, DHCPv6 Relay, IPv4 to IPv6 translations & encapsulations.
11	System Management & Configuration	Using web GUI/client based (without any limitation in number of clients), Command Line Interface (console/telnet/SSH).
12	Supporting Protocols	FTP, **SFTP**, SMTP, HTTP, HTTPS

12	Supporting Protocols	SNMP, UDP, ICMP, RPC, DNS, DHCP, ARP, TCP, POP3, IGMP, PIM.
13	Authentication Protocols	RADIUS, LDAP methods.
14	Routing Protocols	Static, RIP, OSPF, OSPFv3 and BGP, BGPv6.
15	Content Filtering	JAVA & ActiveX blocking.
16	Proposed FW shall also support	a. DoS & DDoS prevention. b. TCP reassemble for fragmented packet protection. c. Brute Force attack mitigation. d. SYN cookie protection. e. Zone/Interface based IP spoofing. f. Malformed packet protection. g. Stateful packet inspection. h. Detail logging and packet capture. i. Antivirus, anti-worm, anti-spam and anti-spyware protection.
17	Filtering	Filtering of packets based on Source address, destination address, protocol type, user, port number, URL (**including URL blocking**).
18	Threat Intelligence	The Appliance OEM must have its own threat intelligence analysis center and should also use the global footprint of security deployments for more comprehensive network protection.
19	Endpoint Quarantine Capability	Solution should support the capability to quarantine/block endpoint traffic by integrating with threat feeds from other security solutions like Network Admission Control. If provisioning of additional licensing is required, same may be considered.
20	Interface Requirement	a. Minimum number of 1 Gbps LAN ports – **4** b. Minimum number of 10 Gbps ports – **12** c. Separate HA port. All SFP+ ports shall have compatible transceivers (Short Range Transceivers) along with required FO cables.
21	Operational Readiness	All features in the firewall should be functional/operational within 5 minutes of Power ON.
22	Policy Deployment Time	Any new policy/policies should be applied in the firewall in not more than 5 minutes. The time shall be measured from the pushing of the policy from the pushing of the policy from management console to the policy becoming effective.
23	End-of-Life (EOL) and End-of-Support (EOS) for 7 years as per TS	
	Support for Patches for 7 years as per TS	
24	Power Supply (in Watts)	----
25	Heat Load	----

Note: - Contractor to ensure

Centralized Management of Firewalls

Sl. No.	Minimum Required Specifications
1	The Firewall Management Solution shall provide dedicated centralized management for central configuration, provisioning, real-time monitoring, fault management, logging and customized reporting with capability to create scheduled reports. The management platform shall be accessible through web-based interface and/or client-based GUI without any limitation on the number of management clients. All OEM firewalls shall be managed centrally through a single software platform. In case of software-based deployment, all required VM, operating system, database, software installation and configuration required to make the solution operational shall be provided by the contractor. All necessary licenses shall be included in the scope. In case appliance-based management is proposed, all hardware, software and licensing requirements shall be included by the contractor.
2	The management platform must support role-based multi-user management.
3	The management platform must provide centralized logging and reporting functionality.
4	The management / logging platform must be capable of integrating with API for Automation and Orchestration.
5	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
6	For troubleshooting packet tracer/debugging and capture are the two primary capabilities needed.
7	Should support REST API for monitoring and config programmability
8	The management platform must provide multiple report output types or formats, such as PDF and CSV.
9	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
10	Logs must be available for at-least six months, hardware sizing may be considered accordingly.
11	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
12	The management platform support running on-demand and scheduled reports
13	The management platform must risk reports like advanced malware, attacks and network
14	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools. All licenses required for above mentioned security solution must be activated from day one.
15	Same OEM Firewalls located at main and back-up control centre shall be configured and managed by centralised management system located at both locations i.e., main and backup control centre. So that if there is problem in main control centre then all the firewalls from same OEM at both locations shall be managed centrally from backup control centre and vice versa.

5.12 Centralized Management Console

All necessary hardware & software for Web Servers with firewalls and HIDS/NIPS shall be installed by the contractor. A separate Computer shall be supplied to be used as centralized management console for the HIDS/NIPS and firewall. The management console shall perform the following functions:

• Create and deploys new policies

• Collect and archive audit log for post event analysis

• Maintain an integrated event database

• Provide an integrated reporting system.

• Performance monitoring

5.13 Color Laser Printer

The Color Laser Printer shall be suitable for printing AMR system reports, energy accounting reports, dashboards, billing-related documents, technical reports, drawings, and general office documents. The printer shall support high-speed network printing with duplex functionality and secure printing features.

Sl. No	Description of the Features	Minimum Quantity of the features	Offered by the Contractor
1.	Manufacturer	----	
2.	Model No.	----	
3.	Functions	Print, scan, email, **copy**	
4.	Paper size	A3, A4	
5.	Print speed	30 Colour pages/minute of A4 size & 15 Colour pages/minute of A3 size.	
6.	Print resolution	1200 × 1200 dpi	
7.	Paper weight	75-200 GSM	
8.	First page out time	10 sec for black and white and 15 sec for colour	
9.	Duty cycle	100000 pages per month	
10.	Paper handling capacity	Minimum 500 sheets for input tray & 500 sheets for output tray.	
11.	Automatic duplex printing	Yes	
12.	Landscape and portrait orientation	Yes	
13.	RAM	1500 or more MB	
14.	Hard Disk Capacity	256 GB	
15.	Interface	Dual 1GB internal LAN ports (**2nd Port could be Print Server**)	
16.	Heat Load	----	

5.14 Communication Accessories like L2 Switches

i. 16 ports Industrial grade layer 2 Ethernet Switch, 12 number 10/100/1000 MBPS RJ 45 ports & 4 numbers 1/10G FO Port at Substation Control room.

ii. Industrial grade layer 2 Ethernet Switch with required RJ 45 ports and FO ports at Switchyard location to convert electrical data to optical.

iii. AC (240V) or DC (110V/220V) power supply with rack or DIN or Panel Mountable Hardware

iv. Minimum 2 no spare ports in each switch shall be ensured during implementation.

Note- Number of ethernet switch at each station shall be as per requirement during detailed engineering.

5.15 Furniture

5.15.1 Workstation Desk: Motorized

Each workstation shall be provided with a suitable desk as follows:

a. Sectional frame suitably clad with hardwood or hard wearing material.
b. Desktops of a durable, scratch resistant, non-reflecting finish of suitable thickness.
c. Proper Channels for Power, LAN and Telephone cabling with 100% spare capacity i.e., integrated cable management system shall be in place.
d. Adequate space shall be provided on the desktop for the writing area, to accommodate the operator workstation, mouse, telephone and other miscellaneous items.
e. Drawers, shelves, and miscellaneous fittings. Access shall be allowed for maintenance to equipment mounted on or in the desk. Pull out Drawer, Doors or removable panels shall be provided for this purpose.
f. Adjustable (height) desks (sit-and-stand with step-less automatic height adjustment).
g. Independent electronic powered height adjustment of monitors platform and workspace.
h. Table shall have been provided with sufficient number of power sockets, LAN ports, door-lights, sliding trolley for CPU, soft-door closure etc. Number of sliding trollies, LAN port and power sockets may be provided as per the owner additional requirement.
i. All bolts shall be of SS material to avoid rust due to environment.

5.15.2 Workstation Desk: Normal / U-Type

Each workstation shall be provided with a suitable desk as follows:

a. Sectional frame suitably clad with hardwood or hard wearing material.
b. Desktops of a durable, scratch resistant, non-reflecting finish of suitable thickness. Proper Channels for Power, LAN and Telephone cabling with 100% spare capacity i.e.
c. Integrated cable management system shall be in place.
d. Adequate space shall be provided on the desktop for the writing area, to accommodate the operator workstation, mouse, telephone fand other miscellaneous items.
e. Drawers, shelves and miscellaneous fittings.
f. Access shall be allowed for maintenance to equipment mounted on or in the desk. Pull out Drawer, Doors or removable panels shall be provided for this purpose.
g. Table shall have been provided with sufficient number of power sockets, LAN ports, door-lights, sliding trolley for CPU, soft-door closure etc. Number of sliding trollies, LAN port and power sockets may be provided as per the owner additional requirement.

h. All bolts shall be of SS material to avoid rust due to environment.

5.15.3 Chairs

a. Two chairs shall be provided at each workstation.
b. The chair shall be of high-backed design with arm rests, covered in durable woven material.
c. The chairs shall be of good quality and suitable for continuous use without discomfort.
d. Pneumatic Seat height and back angle adjustments shall be provided, capable of easy operation.

5.16 Time Synchronisation Equipment

i. The Time synchronization equipment shall receive the coordinated Universal Time (UTC) transmitted through Geo Positioning Satellite System (GPS) / NAVIC and synchronize equipments to the Indian Standard Time in a substation.
ii. Time synchronization equipment shall include antenna, all special cables and processing equipment etc.
iii. It shall be compatible for synchronization of IEM & DCU, at a substation through individual port or through Ethernet
iv. Equipment shall operate up to the ambient temperature of 50 degree centigrade and 80% humidity.
v. The synchronization equipment shall have 1.5 micro-second accuracy. Equipment shall give real time corresponding to IST (taking into consideration all factors like voltage, & temperature variations, propagation & processing delays etc).
vi. The system shall be able to track the satellites to ensure no interruption of synchronization signal.
vii. The output signal from each port shall be programmable at site for either one hour, half hour, minute or second pulse, as per requirement.
viii. The equipment offered shall have four (04) output ports. Various combinations of output ports shall be selected by the customer, during detailed engineering, from the following:
• IRIG-B
• SNTP Port
ix. The equipment shall have a periodic time correction facility of one second periodicity.
x. Time synchronization equipment shall be suitable to operate from AC (240V) or DC (110V/220V) power supply as available at Substation.
xi. Equipment shall have real time digital display in hour, minute, second (24 hour mode)

5.17 Various Power and Communication Accessories

1. General Requirements

The bidder shall provide all armoured power cables, networking cables, connectors, mounting accessories, termination hardware, software utilities, consumables, and miscellaneous items required for complete installation, testing, commissioning, integration, and successful operation of the AMR System. All accessories shall be of industrial/enterprise grade and sourced from reputed OEMs.

2. Power Distribution Components

- Armoured Copper power cables of suitable rating for all supplied equipment.

- Miniature Circuit Breakers (MCBs) of appropriate ratings.
- Power sockets, plugs, terminal blocks, cable glands, ferrules, and lugs.
- Rack Power Distribution Units (PDUs).
- Earthing and grounding accessories.
- Surge protection devices as required.

3. Network Cabling Components

- CAT-6/CAT-6A UTP/SFTP Ethernet Cables.
- CAT-6/CAT-6A Information Outlets and RJ45 Jacks.
- RJ45 Connectors and Termination Accessories.
- CAT-6 Patch Panels.
- Factory-terminated Patch Cords of suitable lengths.
- Cable Managers, Cable Ties, Labels, and Identification Tags.

4. Fiber Optic Components

- Single Mode Fiber Patch Cords.
- Fiber Connectors, Adapters, and Pigtails.
- SFP/SFP+ Modules where required.
- Fiber Management and Routing Accessories.

5. Mounting and Installation Accessories

- Rack Mounting Hardware.
- Cable Trays, Raceway Accessories, and Cable Ducts.
- Mounting Brackets, Fasteners, Screws, Nuts, and Bolts.
- Equipment Labels and Nameplates.
- Cable Markers and Identification Accessories.

Item wise detail of each material shall be finalised during detail engineering and site survey.

5.18 Intrusion Detection & Prevention System

The required features of the Host Based Intrusion Detection and Prevention System (HIPS) and Network Based Intrusion Detection Prevention System (NIPS) are described below:

a) Intrusion Detection and Prevention System (Host Based)

Host based Intrusion Detection and Prevention System module shall be provided for all machines on DMZ LANs and machines interacting from outside the network. IDS shall be able to perform following actions:

- Capability for Detecting the intrusion attempt that may take place, intrusion in progress and the intrusion that has taken place.
- Flag and check unauthorized access
    - Notify/Alarm/message of intrusion to:
    - Management console
    - Event log
    - Administrator by e-mail
- Create an audit trail for user and file access activity, including file accesses, changes to file permissions, attempts to install new executables and/or attempts to access privileged services
- In an event where user accounts are added, deleted, or modified, changes to key system files and executables is done by unauthorized account or there is an unauthorized attempt

to overwrite vital system files, to install Trojan horses or backdoors, suitable action should be taken such as:
    - Terminate User (intruder) directly or through Active directory, SIEM etc.
    - Login Disable User (intruder) Account directly or through Active directory, SIEM etc.
    - Forge a TCP FIN packet to force intruder connection to terminate
- Shall provide events check for suspicious file transfers, denied login attempts, physical messages (like an Ethernet interface set to promiscuous mode) and system reboots etc.

b) Network based Intrusion Prevention System (NIPS)

The NIPS shall provide complete inline protection from network-based application layer threats by scanning packet payloads for malicious traffic. It shall detect, classify and stop malicious application, viruses, worms and spyware/adware etc. After detecting an intrusion attempt NIPS should be able to perform following actions:

- Suggest/Reconfigure changes in the firewalls provided in this package
- Send an SNMP Trap datagram to the management console.
- Send an event to the event log.
- Send e-mail to the administrator to notify the attack.
- Save the attack information (timestamp, intruder IP address, victim IP
- address/port, protocol information)
- Force intruder connection to terminate.
- NIPS shall have capability to detect various operating system of devices/servers running on the network and profile them for more visibility and protection (for impact assessment & vulnerability analysis)

5.19 Security Information and Event management (SIEM)

A dedicated system called SIEM shall be deployed having following features:

- SIEM tool shall offer a single, unified view for all logs generated across the AMR network.
- As per CEA 2026 regulations, SIEM shall store 180 days of logs of all devices and systems including applications, network activities etc.
- The contractor shall ensure that the logs associated with an incident including logs pertaining to one hundred and eighty days prior and post to such incident are available for at least one hundred and eighty days from occurrence of such incident.
- SIEM system shall be easy to install, configure, use and maintain.
- SIEM shall have pre-built dashboard containing statistical information about the complete system. There shall be a feature to create customized dashboards to organize and correlate multiple data sources visually in a single user interface.
- Complete network-based scanning enabling assessment and analysis of threats impacting network.
- Log collection (EPS) to be maintained as: Sustained EPS-15000, Peak EPS-18000, Burst EPS-22500 with response <30 sec.
- Robust Log data warehouse that enables creation and sharing of reports on all aspects of the system's remediation efforts in support of policy compliance.
- Create custom remediation packages to address recurring configuration issues, remove unauthorized files and applications, and patch software.

- Configurable monitoring to enable Regulatory and standards-based assessment of end points compliance
- Continuous Monitoring - continuously collect detailed status information on all critical cyber assets and immediately detect any changes.
- Automated Assessment - automatically aggregate and analyze security data and raise alert on suspicious events or modifications that impact compliance status.
- Audit-ready Evidence - Quickly generate reports and update dashboards that provides transparent overview of the systems by requirement, compliance with security controls and processes.
- SIEM solution shall be able to integrate with all security solutions provided including Firewall, Server security and Endpoint security solutions through standard protocols.
- The solution shall be able to not only detect threat but also shall be able to recommend appropriate response.
- SIEM shall use a variety of advanced detection and investigative controls to detect abnormal activity which is often associated with any compromised systems.

5.20 Expandability and Scalability

The AMR System hardware, software and associated Control Centre Infrastructure shall be designed with sufficient scalability to accommodate a minimum growth of **50% over the initial sizing specified in Section 5.7** without requiring significant architectural modifications or causing degradation of system performance. The contractor shall demonstrate the scalability feature during FAT.

The infrastructure shall be sized to support acquisition, storage, processing and management of metering data from approx. 13765 Interface Energy Meters (IEMs) as per BOQ, including 5-minute energy data, 1-minute MW data, event logs, diagnostics data, communication logs and other associated data, along with the specified future growth requirements.

Chapter 6 — Software Requirements and Cyber Security

6.1 General Software Requirements

AMR system software shall be built on a Standard database management solution platform, supporting archival and retrieval of data, with a browser/console-based client interface and reports available in PDF, standard spreadsheet, CSV and text formats. Operating system and application software shall be fully upgradable by firmware or software upgrade methods, with every such upgrade logged in the system. Licenses of all Software shall be provided by the contractor in the name of employer with its validity till completion of AMC period.

6.2 Technical Specifications for Software

A. Reporting & Dash Boarding System

The AMR solution shall provide a comprehensive web-based Reporting and Dashboarding System for monitoring meter data acquisition performance, data quality, communication health, events, alarms, and energy data analytics. The system shall include a set of standard reports along with user-configurable report generation capabilities.

i. Standard Reports

The system shall provide, at a minimum, the following reports:

- Meter communication exceptions.
- Data validation and quality check reports.
- Meter installation, replacement, addition, and removal reports.
- Meter inventory reports.
- Defective/non-communicating meter reports.
- AMR system performance and availability reports.
- Meter-wise, substation-wise, region-wise and utility-wise reports.
- Weekly meter data acquisition status reports.
- Meter polling success and failure reports.
- Time synchronization exception reports.

ii. Custom Reporting

- Users shall be able to modify standard reports and create customized reports without requiring software source-code modifications.
- Report generation shall be GUI-based using user-selectable filters, parameters, and drop-down menus.
- The system shall support ad-hoc query generation and customized analytics reports.
- Query creation and report configuration shall not require proprietary programming knowledge.

iii. Report Output and Distribution Reports shall be exportable in standard formats including:

- PDF
- Microsoft Excel
- CSV
- Word

The system shall support:

- Scheduled report generation.
- Automatic email distribution.
- Storage of reports in configurable network directories.
- Printing and archival of reports.

iv. **Dashboard Features** The dashboard shall provide graphical and tabular visualization of:
- Meter communication status.
- Data acquisition success percentage.
- Missing data statistics.
- Event and alarm summaries.
- Communication performance trends.

The dashboard shall support graphical representation through bar charts, trend charts, pie charts, gauges, heat maps, and KPI indicators.

v. **Interface Monitoring Reports** The system shall provide weekly interface exception reports for data sharing with MDP system of RLDC

The reports shall identify data transfer failures and missing records

B. Database Software (DB)

Initial Database Generation

The contractor shall be responsible for the initial database creation, configuration, migration, and population using meter inventory, communication network details, user information, hierarchy data, and other information provided by the Employer. The contractor shall verify the correctness and completeness of the data before commissioning.

Database Development Tools

The contractor shall provide all necessary software tools for development, administration, maintenance, backup, and monitoring of the AMR database. The tools shall support:

- Creation, modification, import, and export of database objects and records.
- Full and incremental data import/export.
- Export of data in standard formats such as XML, CSV, JSON, and SQL.
- Database migration and integration with third-party systems.
- Database schema management and version control.
- Support for interoperability with databases and applications from different vendors.

Database Management

The database management system shall support:

- Data insertion, retrieval, update, and deletion.
- Indexing, partitioning, and query optimization.
- Management of meter data, events, alarms, audit logs and configuration data.
- Database integrity and consistency checks.
- Online backup and recovery operations.
- Distributed database access, where applicable.
- Online database maintenance without interruption to AMR operations.

- Creation, modification, and resizing of database structures and storage allocation.
- Addition and modification of database attributes and objects.

Database administration activities shall not adversely affect normal AMR data acquisition, processing, reporting, or dashboard functions.

Audit Trail and Change Tracking

The database system shall maintain audit trails for all database changes, including:

- Addition, modification, and deletion of records.
- Database configuration changes.
- User account changes.
- Data import/export activities.

Each audit entry shall record:

- User ID
- Date and time stamp
- Activity performed
- Old and new values (where applicable)

The system shall maintain an audit history of at least the last **10,000 change transactions** or as per database retention policy.

Integration

The database shall support secure data exchange with:

- AMR Application
- Reporting & Dashboarding System
- Asset Management Systems

The database shall support data exchange through standard interfaces such as SQL, ODBC, JDBC, REST APIs, XML, JSON, and CSV formats.

C. Operating System

The operating system of all the equipment of AMR system including network equipment shall be latest version released up to six months prior to FAT. The operating system shall be hardened to provide robust security.

In order to facilitate cyber security requirements including patch management, common operating system is preferable to be used by all server nodes within the AMR. This is also to minimize the maintenance. All licences for Operating System and other application software shall be supplied by the contractor and shall be valid throughout the operating life.

D. Backup & Restore Software

The contractor shall provide all software tools and utilities required for backup, recovery, monitoring, maintenance, data exchange, and administration of the AMR system, databases, applications, and servers.

- The solution shall provide automated backup and restoration facilities for AMR applications, databases, configuration files, reports, dashboards, logs, and operating system images.
- Backup data shall be stored on NAS or other designated storage media.
- The system shall support full, incremental, and differential backups at user-configurable intervals.
- Backup retention shall be configurable, with support for long-term archival up to 7 years.
- Backup policy shall be implemented to ensure that online or offline backup data or both, as applicable, of all critical systems is up to date, but not older than a month, and retained in a separate and safe environment for the period as specified in the data retention policy.
- It shall be ensured that at least last two working data backups are available.
- The Vendor shall provide documented and periodically tested recovery procedures and disaster recovery plans for all supplied systems to enable restoration from cyber incidents and cyber crisis situations.
- Users shall be able to select files and databases for backup based on:
    - Server/workstation
    - File name or directory
    - Creation/modification date
    - Changes since previous backup
- The solution shall support bare-metal recovery through system image backups of servers and workstations.
- It shall be possible to restore the AMR application, database, or server configuration to a user-selected recovery point.
- Backup and restoration activities shall not affect normal AMR operations.

E. Host Based IDS (Intrusion Detection System) for all machines

Host based Intrusion Detection System module shall be provided for all machines. IDS shall be able to perform following actions:

- Capability for Detecting the intrusion attempt that may take place, intrusion in progress and the intrusion that has taken place.
- Flag and check unauthorized access
- Notify/Alarm/message of intrusion to:
- Management console
- Event log
- Administrator by e-mail
- Create an audit trail for user and file access activity, including file accesses, changes to file permissions, attempts to install new executables and/or attempts to access privileged services
- In an event where user accounts are added, deleted, or modified, changes to key system files and executables is done in by unauthorized account or there is unauthorized attempt to overwrite vital system files, to install Trojan horses or backdoors suitable action should be taken such as:
    - Terminate User (intruder) Login
    - Disable User (intruder) Account
    - Forge a TCP FIN packet to force 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.

F. Software for Data Replica Server

The contractor shall provide Data Replica Server software for maintaining a synchronized copy of the AMR application database, meter data repository, configuration data, reports, and system logs for backup, business continuity and reporting purposes.

Functional Requirements

- The Data Replica Server shall maintain an up-to-date replica of the primary AMR database through automatic data synchronization.
- The replication mechanism shall support real-time or scheduled synchronization with configurable intervals.
- The solution shall support replication of:
    - Meter data
    - Event and alarm data
    - Configuration data
    - User and audit logs
    - Reports and dashboards
- Replication shall be automatic and shall not require manual intervention.

Replication Features

- Support full and incremental data replication.
- Support database-level and file-level replication.
- Support bidirectional or unidirectional replication, as required.
- Data consistency and integrity checks shall be performed during synchronization.
- Replication failures shall be automatically detected and logged.
- Automatic re-synchronization shall be initiated after restoration of communication.

Monitoring & Administration

- Real-time monitoring of replication status shall be available through a web-based dashboard.
- The system shall generate alarms for:
    - Replication failure
    - Synchronization delays
    - Database connectivity issues
    - Storage utilization thresholds
- Replication logs and audit trails shall be maintained for analysis and troubleshooting.

Security

- Replication data shall be encrypted during transmission.
- Access to replication management functions shall be role-based.
- Audit logs shall record all replication-related activities and configuration changes.

Integration

- The Data Replica Server shall be fully integrated with the AMR application, database, reporting system, and backup infrastructure.

- The replica database shall be available for reporting, analytics, and disaster recovery purposes without impacting the performance of the primary AMR system.

Scalability

- The replication solution shall support the complete AMR database and future expansion of at least 50% of the initially configured meter population without requiring replacement of the replication platform.

G. Software Centralised Management Console

The contractor shall provide a Centralized Management Console (CMC) for unified monitoring, administration, configuration, security management, reporting, and maintenance of the complete AMR infrastructure. The CMC shall provide a single web-based interface for managing AMR applications, communication equipment, meters, servers, databases, storage systems, and cybersecurity components.

Functional Requirements

The Centralized Management Console shall provide:

- Centralized monitoring of all AMR system components.
- Consolidated view of meter communication status, server health, database status, storage utilization, and network performance.
- Centralized configuration and administration of AMR system parameters.
- User and role management with Role-Based Access Control (RBAC).
- Alarm, event, and notification management.
- Centralized audit trail and activity logging.
- Asset inventory management for meters, communication devices, servers, and software components.
- Dashboard-based visualization of system performance and operational KPIs.

Monitoring and Management Features

The CMC shall support monitoring of:

- AMR application servers.
- Databases and Data Replica Servers.
- Communication gateways and network devices.
- Meter communication status.
- Data acquisition performance.
- Storage devices and backup systems.
- Application services and processes.
- Cybersecurity events and system alerts.

Dashboard and Reporting

The CMC shall provide configurable dashboards displaying:

- Total configured meters.
- Communicating and non-communicating meters.
- Data acquisition success rate.

- Communication network health.
- Active alarms and events.
- Server and database health status.
- Storage and backup utilization.
- System performance statistics.

Reports shall be exportable in PDF, Excel, CSV, and Word formats.

Alarm and Notification Management

The system shall:

- Generate alarms for communication failures, hardware faults, database issues, security events, and application failures.
- Support alarm prioritization and categorization.
- Provide notifications through email, SMS, and web dashboards.
- Maintain historical alarm and event records.

Security Features

The CMC shall support:

- HTTPS-secured access.
- Role-based user access control.
- Audit logs for all user activities and configuration changes.
- Password policy enforcement.
- Session timeout and account lockout features.

Integration

The Centralized Management Console shall support integration with:

- AMR Application
- Reporting & Dashboarding System
- Database Software
- Data Replica Server
- Backup & Restore System
- Meter Data Management System (MDMS)
- Billing and Energy Accounting Systems
- Network Management and Cyber Security Systems
- through standard APIs, Web Services, XML, JSON, and database interfaces.

Availability and Scalability

- The CMC shall support centralized management of the entire AMR deployment from a single console.
- The solution shall support a meters as per project scope initially with provision for 50% future expansion.
- Addition of new meters, communication devices, servers, and applications shall not require replacement of the management platform.

H. Web Server System Software

The contractor shall provide Web Server System Software for hosting and delivering web-based access to the AMR application, dashboards, reports, administration portals, APIs, and associated services. The web server shall provide secure, reliable, and high-performance access to authorized users through standard web browsers without requiring additional client software.

Functional Requirements

- Provide browser-based access to AMR dashboards, reports, meter data, alarms, and system administration functions.
- Support concurrent access by multiple users without performance degradation.
- Support centralized user authentication and authorization.
- Host AMR application services, web portals, APIs, and reporting interfaces.
- Support secure communication between clients, application servers, and databases.

Supported Features

- HTTPS-secured web access.
- Support for HTML5-compatible web browsers.
- Role-Based Access Control (RBAC).
- Session management and user activity tracking.
- Dashboard and report visualization.
- Web-based configuration and administration.
- REST API and Web Service hosting.
- File upload and download facilities.
- Audit logging of user activities.

Security Requirements

- TLS 1.2/1.3 encrypted communication.
- Integration with Active Directory (AD) and LDAP.
- Password policy enforcement.
- Account lockout mechanism.
- Session timeout management.
- Protection against common web vulnerabilities.
- Audit trail of login, logout, configuration changes, and report generation activities.
- Support for Multi-Factor Authentication (MFA) preferably.

Performance and Availability

- Support 24×7 continuous operation.
- Load balancing and clustering support (preferred).
- High availability and failover capability.
- Automatic service restart and recovery mechanisms.
- Real-time health monitoring and alert generation.

Integration

The Web Server shall support integration with:

- AMR Application
- Centralized Management Console
- Reporting & Dashboarding System
- Database Server
- Data Replica Server

through standard APIs, Web Services, XML, JSON, and database interfaces.

Compatibility

The Web Server System Software shall be compatible with:

- Windows Server and Linux operating systems.
- Major web browsers including Microsoft Edge, Google Chrome, and Mozilla Firefox.
- Standard enterprise databases such as Oracle, PostgreSQL, SQL Server, and MySQL.

I. Antivirus Software

All computers and firewalls shall be provided with the latest antivirus software as on date of supply. The antivirus software shall have the capability of having its virus definitions updated from time to time. The Contractor shall be responsible for the maintenance & update of the antivirus software during AMC period without any extra cost to employer.

J. Identity and Patch Management Software

The contractor shall provide Identity and Patch Management Software for centralized management of user identities, access privileges, authentication mechanisms, endpoint security, software updates, security patches, and compliance monitoring across the complete AMR infrastructure.

Functional Requirements

The software shall provide:

- Centralized identity and access management for all AMR users, administrators, and service accounts.
- Centralized deployment and management of operating system, application, database, and security patches.
- Policy-based access control and user provisioning.
- Authentication, authorization, and account management.
- Security compliance monitoring and reporting.
- Automated patch distribution and installation.

Identity Management Features

The solution shall support:

- Role-Based Access Control (RBAC).
- User and group management.
- Centralized authentication and authorization.
- Integration with Active Directory (AD) and LDAP.
- Single Sign-On (SSO) support (preferred).
- Multi-Factor Authentication (MFA) support.

- Password policy enforcement.
- Account lockout and session timeout mechanisms.
- Automated user provisioning and de-provisioning.
- Audit logging of all user activities.

Patch Management Features

The solution shall support:

- Centralized patch management for servers, workstations, and AMR applications.
- Automated discovery of software and operating system versions.
- Vulnerability assessment and patch compliance monitoring.
- Deployment of operating system, database, antivirus, firmware, and application updates.
- Scheduled patch deployment during user-defined maintenance windows.
- Patch testing, approval, rollback, and recovery mechanisms.
- Verification of successful patch installation.
- Generation of patch status and compliance reports.

Monitoring and Reporting

The software shall provide dashboards and reports for:

- User login and access activities.
- Privileged account activities.
- Authentication failures and security violations.
- Patch deployment status.
- Missing security patches.
- Compliance status of servers and endpoints.
- Security and vulnerability trends.
- Audit trail and change management records.

Reports shall be exportable in PDF, Excel, CSV, and Word formats.

Security Requirements

The software shall:

- Support encrypted communication using HTTPS/TLS.
- Maintain audit logs of all identity and patch management activities.
- Generate alerts for unauthorized access attempts and non-compliant systems.
- Support compliance with organizational cyber security policies and CERT-In guidelines.
- Provide secure storage of credentials and security policies.

Integration

The solution shall support integration with:

- AMR Application
- Centralized Management Console
- Web Server System
- Database Server

- Data Replica Server
- Antivirus/Endpoint Protection System
- SIEM/SOC Platforms
- Active Directory and LDAP Services

through standard APIs and secure interfaces.

Availability and Scalability

- Support centralized administration of the complete AMR infrastructure.
- Operate without interruption to normal AMR services during monitoring and patch deployment activities.
- Support future expansion of users, servers, workstations, applications, and network devices without requiring replacement of the platform.

K. Software For Network Attached Storage (NAS)

The contractor shall provide all software, licenses, utilities, and management tools required for operation, monitoring, administration, security, backup, and maintenance of the Network Attached Storage (NAS) system deployed as part of the AMR infrastructure.

Functional Requirements

The NAS software shall provide:

- Centralized storage management for AMR applications, databases, reports, logs, backups, and historical meter data.
- Web-based administration and monitoring interface.
- File sharing and storage services over standard network protocols.
- Storage allocation, volume management, and capacity expansion without service interruption.
- Multi-user concurrent access with role-based permissions.
- Automated storage utilization monitoring and reporting.

Storage Management Features

The software shall support:

- Creation, modification, and deletion of storage volumes and file systems.
- RAID configuration and management.
- Online storage expansion.
- Snapshot creation and management.
- Data replication and synchronization.
- Quota management for users and applications.
- Archiving of historical data.
- File compression and deduplication (preferred).

Backup and Recovery

The NAS software shall support:

- Full, incremental, and differential backups.

- Automatic backup scheduling.
- Snapshot-based recovery.
- File-level and volume-level restoration.
- Long-term backup retention as per utility requirements.
- Backup and recovery without impacting normal AMR operations.

Monitoring and Reporting

The software shall provide:

- Real-time storage health monitoring.
- Capacity utilization monitoring.
- Disk health and performance monitoring.
- RAID status monitoring.
- Alert generation for hardware failures, storage thresholds, and backup failures.
- Historical performance and usage reports.
- Email notification of critical events and alarms.

Security Features

The software shall support:

- Role-Based Access Control (RBAC).
- Active Directory (AD) / LDAP integration.
- User authentication and authorization.
- Data encryption at rest and in transit.
- Audit logs for all administrative activities.
- HTTPS/TLS secure management access.
- Password policy enforcement.
- Ransomware protection and secure snapshot features (preferred).

Integration

The NAS software shall support integration with:

- AMR Application
- Database Server
- Data Replica Server
- Backup & Restore Software
- Centralized Management Console
- Reporting & Dashboarding System

through standard protocols such as SMB/CIFS, NFS, FTP/SFTP, Rsync, SNMP, and REST APIs.

Availability and Scalability

- Support 24×7 continuous operation.
- Support hot-swappable disk replacement.
- Support redundant storage architecture and failover mechanisms.
- Support future storage expansion without replacement of the NAS platform.
- Support minimum 10 TB usable storage capacity with provision for future expansion.

L. Data Historian Software

1.1 General Requirements

The Data Historian Software shall provide centralized acquisition, storage, archival, retrieval, analysis, and reporting of all AMR system data collected from Energy Meters, DCUs, Gateways, RTUs, and other data sources.

The Historian shall be designed for handling large volumes of time-series metering data and support historical data retention for a minimum period of seven (7) years.

The system shall support scalable architecture capable of handling future expansion without performance degradation.

1.2 Data Acquisition

The Historian shall acquire and store data received from:

- Interface Meters
- DCUs/Gateways
- AMR System
- External applications through APIs

Audit records shall not be editable.

M. Software For Development Server For Testing And Training

Remote Diagnostic facility with necessary hardware as required shall be provided for communication between the AMR system at control center and the Contractor`s & Employer support office for the diagnosis of hardware & software problems. The login shall be protected by a user name & password entry. An automatic intimation shall be provided to inform authorized person from utility on such events of remote access and diagnosis.

Development System as a Test Bench

Development system shall be able to provide testing facility for integration of new AMR devices before putting it online with Real-time system.

The contractor shall provide a separate Development, Testing and Training Environment for the AMR system to facilitate application development, configuration changes, software upgrades, testing, user acceptance testing (UAT), cybersecurity validation, training, and demonstration activities without impacting the operational AMR system.

Functional Requirements

- The Development Server shall replicate the operational AMR environment for testing and validation purposes.
- The environment shall support development, testing, debugging, and evaluation of new functionalities, reports, dashboards, interfaces, and software upgrades.
- The testing and training environment shall be logically isolated from the production environment.
- Changes shall be validated in the Development/Test environment prior to deployment in the production system.

- The system shall support creation of test databases using anonymized or replicated production data.

Testing Features

The Development Server shall support:

- Functional Testing.
- Integration Testing.
- User Acceptance Testing (UAT).
- Interface and API Testing.
- Performance Testing.
- Security and Vulnerability Testing.
- Patch and Upgrade Validation.
- Backup and Restore Testing.

Training Features

The training environment shall support:

- User training for administrators, operators, and engineers.
- Simulation of meter data acquisition, events, alarms, and communication failures.
- Demonstration of reports, dashboards, analytics, and system administration functions.
- Role-based access for training users.
- Reset and restoration of training data without affecting production data.

Data Management

- The Development Server shall support import and export of configuration, reports, dashboards, and databases.
- Test data generation utilities shall be provided.
- Periodic synchronization of selected master data from the production environment shall be supported.
- All test activities shall be isolated from live AMR operations.

Integration

The Development, Testing and Training Environment shall support integration with:

- AMR Application
- Database Server
- Reporting & Dashboarding System
- Data Historian
- Centralized Management Console
- External APIs

for validation of interfaces and functionality before deployment to the production system.

Licensing

All software licenses, development tools, testing utilities, simulation tools, training modules, databases, connectors, and administrative software required for successful operation of the Development, Testing and Training Environment shall be included in the contractor's scope

N. Email Software

The contractor shall provide Email Software and associated services for automated delivery of system notifications, alarms, reports, alerts, audit information, and operational messages generated by the AMR system. The solution shall support secure integration with the utility's corporate email infrastructure and facilitate automated communication with authorized users.

Functional Requirements

The Email Software shall support:

- Automated email generation and delivery from all AMR modules.
- Distribution of alarms, events, exceptions, reports, and system notifications.
- User-configurable email recipients, distribution groups, and mailing lists.
- Scheduled and event-driven email notifications.
- Support for attachments including PDF, Excel, CSV, Word, and image files.
- Configurable email templates and message formats.

Notification Features

The system shall support email notifications for:

- Communication failures.
- Non-communicating meters.
- Missing meter data.
- User account and access management events.
- Scheduled report delivery.

Integration

The Email Software shall support integration with:

- AMR Application
- Reporting & Dashboarding System
- Historian System
- Centralized Management Console
- Database Server
- Identity and Patch Management System

Security Requirements

The solution shall support:

- TLS/SSL encrypted email communication.
- Role-Based Access Control (RBAC).
- Audit logging of email delivery activities.
- Configurable sender policies.
- Protection against unauthorized relay and misuse.

Management and Monitoring

The software shall provide:

- Email delivery status monitoring.
- Message queue management.
- Failed delivery tracking and re-transmission.
- Audit trail of sent emails.
- User-configurable notification rules and escalation mechanisms.

Scalability and Availability

- The solution shall support concurrent email delivery to multiple users and groups.
- Email services shall operate continuously on a 24×7 basis.
- The system shall support future expansion without degradation in performance.

6.3 Cyber Security — Regulatory Framework

The complete IEM/DCU/AMR/MDP chain shall comply with: orders of the Ministry of Power, Government of India, on cyber security; the CEA Cyber Security in Power Sector Guidelines dated 7 October 2021 and subsequent amendments; CERC Regulations; and CERT-In Directions relating to information-security practices, prevention, response and reporting of cyber incidents dated 28 April 2022, as may be updated from time to time (CERT-In guidance is published at https://www.cert-in.org.in). A third-party security audit by a CERT-In-empanelled auditor shall be completed prior to commissioning or Go-Live, whichever is earlier.

6.4 Minimum Cyber Security Measures

1. Hardening of all hardware, operating systems and application software.
2. No application software other than meant for/ required for OT system shall be installed without prior approval of employer/owner.
3. Process controls systems shall be designed, configured, operated, and maintained to provide only required functions. Operating System services and components not required for safe and secure operation of Control System should be disabled / uninstalled. All unused default operating system users shall be disabled.
4. All the Hardware, Operating Systems (OS) and application software shall be hardened based on industry standards and best practices. List of ports and services enabled in each hardware device must be shared after SAT. This list must be updated periodically if any new ports/services are allowed or blocked after prior approval of Owner.
5. Whitelisting policy shall be deployed for all software, services, port configuration, network routing, data flow, access etc. and all these details shall be documented, and any changes shall be recorded and informed to owner during entire period of contract. List of ports and services enabled in each hardware and software must be updated periodically during Maintenance Period if any new ports/services are allowed or blocked after prior approval of Owner.
6. Network partitioning and use of a DMZ/firewall while facilitating data access for RLDC and SLDC users.
7. Mandatory change of all default user IDs and passwords on first login.
8. Logging of all log-in/log-out events and cable plug-in/plug-out events.

9. Role-based authorisation control, limiting each user to functions for which they have been explicitly authorised by the system administrator.
10. Automatic session lock after 30 minutes of inactivity (configurable) for both system and application sessions.
11. Recording of all network traffic for detection of unauthorised or unusual activity and attempts to defeat system security.
12. Explicit identification and minimisation of the network protocols in use for the AMR system, disabling anything not required.
13. Disabling of all unused USB / Bluetooth/WiFi ports on servers/workstations at the AMR control centre.
14. Systems under operation shall not be run in administrator mode in normal operations. Administrator mode should only be used for specific administrative requirements.
15. Transferring information from OT network is to be done only as per approved procedure for secure transfer of data
16. Anti-virus shall be installed in computers and laptops used in OT network. Laptops which are not registered and labelled shall not be connected to OT network.
17. Any software/application/OS which is to be downloaded from OEM's website, its integrity check using hash SHA256 calculation should be done and verified by the contractor before installation.
18. RDP, SMB and other remote administration services shall be disabled where not required and otherwise restricted through approved security controls only within network.
19. Secure digital certificates shall be supported and configured
20. Password Managers shall be used to store passwords in encrypted format and use it to perform any logins into the system.
21. Uniform IP address documents shall be maintained.
22. Login banners with configurable warning text shall be provided for all operating systems.
23. The Contractor shall configure each component of the procured product to operate using the principle of least privilege. This includes operating system permissions, file access, user communications, and system services.
24. All Unused ports (physical and logical) of all devices such as on switches, routers, firewalls, consoles, servers etc. shall be disabled.
25. All unused services shall be disabled by default. There shall be a provision to turn on all services on request.
26. Host-based firewalls shall be configured to only allow connections from specified nodes.
27. All the communication should be done through secure protocols such as SFTP, HTTPS etc. All communication with system constituents shall be encrypted on application level, as applicable.
28. For web-based systems, compliance with OWASP Top 10, API security assessment, and secure session management shall be ensured.
29. Implement proper Access matrix (Access Control List-ACL) to prevent unauthorized access to resources / pages / forms in website.
30. Do not reference components (such as javascripts, stylesheets etc.) directly from third-party sites.
31. Store critical data such as secret keys, passwords, certificates etc. in encrypted form in the database.
32. Disable directory listing.
33. Use the latest and non-vulnerable versions of Application Server (IIS/Apache etc.)

34. Firewalls shall be configured with Clean-up rule: Place a ‘Deny Any-Any’ rule at the end of the rule base. o Never create an ‘Allow any-any’ rule. o Allow rules should be created only for required services.
35. ACLs (Access Control Lists) shall include
36. Apply egress/ingress filter
37. Filter all RFC 1918, 3330 address space and special/reserved address
38. Permit the required services for the required IP addresses only o Deny everything else.
39. Area segregation must be implemented (if OSPF is being used) between internal and external networks. Appropriate protocols must be enabled to prevent networks loops.
40. Cyber Security Guidelines to be followed by Vendor as per CEA regulations 2026.

6.5 Cyber Security Guidelines compliance as per CEA regulations 2026:

1. Provide documented and tested procedures as well as recovery plan to the entity for restoration of systems supplied by them from potential cyber crisis scenarios;
2. Ensure, either digitally signed or validated and authenticated, security patches and updates for all systems as well as components supplied by them are available to the entity throughout their contract period or useful life of such systems, whichever is later;
3. Provide detailed document to the entity consisting of all requirements and processes including security patches as well as updates required to be installed on the third-party components to integrate a component or sub-system supplied by them;
4. Provide details of end of support or end of life of software, hardware and system to the entity, as applicable, supplied by them including those sourced from third parties;
5. Provide Bill of material to the entity, as per Indian Computer Emergency Response Team guidelines issued from time to time, comprising detailed list of all components supplied by them for applications including firmware, deployed in critical systems;
6. The contractor shall ensure that the hardware and software are hardened by enabling all inherent security capabilities, secured configuration, and controls, before supplying to the employer.
7. The Contractor shall adhere to structured vulnerability disclosure program. Patches of the software components shall be provided post completion of the warranty period. These patches shall support offline deployment. Deployment of patches/firmware shall be in the scope of the employer post completion of the warranty period.
8. The Contractor shall establish, document, and maintain approved baseline configurations for all cybersecurity-relevant hardware, software, operating systems, applications, network devices, security appliances, and system components supplied under the Contract. The baseline configuration documents shall be reviewed at least annually and shall be made available for verification during periodic audits conducted by the Employer or its designated auditors.
9. Asset register shall be maintained including its configuration, hardware, software, network architecture depicting data flows and communication protocols used therein.
10. The Contractor shall promptly notify the Employer of any cybersecurity vulnerability, security advisory, exploit, compromise, malware incident, security breach, or cyber incident affecting products, services, software, firmware, or systems supplied under this Contract within six hours of detection and provide detailed RCA and corrective action

11. Such notification shall be made in accordance with applicable Government of India regulations, CERT-In directions, sectoral cybersecurity guidelines, and timelines prescribed by the Employer. The notification shall include impact assessment, mitigation measures, workaround recommendations, and remediation timelines.
12. The Vendor shall provide and maintain an updated Software/Hardware Bill of Materials (SBOM/HBOM), including firmware and third-party components, in accordance with applicable CERT-In guidelines. A sample format with minimum requirement to be filled and supplied by contractor is attached at Appendix-C.
13. The Contractor shall use industry-standard encryption protocols and algorithms, such as [specify encryption standards, e.g., AES-256, TLS 1.2, or higher] for transmitting and storing owners data and information.
14. The Contractor shall implement secure communication channels, such as secure file transfer protocols (SFTP) or virtual private networks (VPNs), for the exchange of sensitive data and information with owner.
15. The Contractor shall maintain and regularly update digital certificates, encryption keys, and other cryptographic materials used for securing communications and data.
16. Contractor shall maintain documented change management procedures for all software, firmware, security patches, configuration changes and cyber security updates with version control, rollback capability and approval records.

    Note:- The model clause of the same is attached as Annexure-C. Same may be referred.

6.6. Cyber Security Audits

The Employer shall engage CERT-In empanelled auditors for conducting Cyber Security Audits, Vulnerability Assessment and Penetration Testing (VAPT), configuration reviews, and compliance assessments during Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT), and throughout the Defect Liability Period and Maintenance Period. The supplied system is also subjected to Audit by Statutory auditors, internal auditors, or any other authorized third-party agency for conducting cyber security audits. The Contractor shall extend all necessary support, assistance, documentation, system access, test environment access, and technical cooperation required for completion of such audits.

Implementation of Audit Recommendations

The Contractor shall implement all applicable observations, recommendations, corrective actions, mitigations, patches, updates, configuration modifications, and remedial measures arising from such audits within timelines mutually agreed upon with the Employer based on the criticality and operational requirements of the system.

Critical and High-risk vulnerabilities identified during cyber security audits shall be remediated within one month and Medium/Low vulnerabilities within three months unless compensating controls approved by Employer are implemented.

The Contractor shall submit a compliance report and closure status against each audit observation/recommendation within the stipulated timeframe. Failure to submit the required compliance report or failure to address agreed audit findings shall constitute a Severity-2 non-compliance under the Contract.

All software updates, security patches, firmware upgrades, configuration changes, and modifications required to address vulnerabilities or audit observations in the products, systems,

applications, and services supplied under the Contract shall be carried out by the Contractor at no additional cost to the Employer.

Where implementation of an audit recommendation necessitates procurement of additional third-party hardware, software licenses, or security appliances not included in the original scope, such items shall be provided by the Employer. The Contractor shall, however, be responsible for integration, configuration, testing, and implementation support thereof.

6.7 Cyber Security Organisation and Governance

The Contractor shall nominate a suitably qualified, ISO 27001-certified Internal Auditor as a single point of contact (SPOC) for all cyber-security matters, responsible for coordinating with the Owner and support-vendor project manager on resolution of cyber-security issues, and for preparing and periodically updating a Risk Assessment/Risk Treatment plan (per ISO 27001) for the project, submitted to the Owner for approval.

6.8 Privacy and Data Protection

The solution provider shall undertake appropriate technical and management measures to minimize the impact of any loss of privacy to a data principal, in line with ISO/IEC 27701:2019, and shall identify, document and classify all privacy-related data, undertaking suitable technical measures in light of applicable law/regulation.

6.9 Monitoring, Reporting and Vulnerability Management

a. Compliance with advisories/alerts from statutory bodies such as NCIIPC and CERT-In shall be ensured within 24 hours of intimation.

b. Half yearly software assurance test and Annual Vulnerability Assessment and Penetration Test (VAPT) shall be conducted for the complete AMR system throughout the AMC period.

Chapter 7 — Annual Maintenance Contract (Operation, Maintenance & Support Service)

7.1 Introduction

The scope of work under maintenance & support services shall include comprehensive maintenance of all the software & hardware (All equipment, peripherals, cables, panels etc. except IEMs) supplied by the contractor for the complete systems along with the future integration and support services for meeting the future requirements envisaged under this project. The maintenance practices to be followed shall be as per ISO 20000 Standard. The essence of the maintenance and support services is to provide maintenance support for the entire system (hardware and software) supplied by the Contractor, with the goal of meeting the availability as set forth herein.

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

7.2 Operation

The contractor shall deploy skilled operating personnel for 24x7 operation at each regional AMR control center to monitor the task scheduler process for data collection, to ensure 100% availability of 5 min load survey data by Tuesday of each week to RLDC & to ensure 1 min instantaneous MW power flow data to SLDCs through secure web browser and also to monitor healthiness of each component of AMR system.

Reporting of failure events (such as. Meter data non-availability, DCU disconnection, communication problem, software/Hardware problems) shall be done automatically by sending mail to the concerned personnel through computer application. There shall be provisions to report breakdown manually with a complaint no. and time. Any defect found by the vendor itself while monitoring shall also be recorded and communicated to the respective Substation in-charge and Employer/Owner.

In case of complete AMR system failure due to server/any other reasons, the contractor shall get 5-minute meter load survey data through mail from all ISTS meter locations in time and manually update the database for further sharing with RLDC.

7.3 Maintenance support

The period of maintenance support shall consist of one-year Warranty (Defect Liability) period (Defect Liability period extendable, if defects found) commencing from Operational Acceptance and six years Maintenance period thereafter.

For any addition (e.g. integration of new IEM or DCU with any AMR control center) during maintenance period, contractor shall provide all the services at control center end as per rate given in BPS during entire period of the contract.

For all third-party equipment (Hardware & Software) Contractor shall have back-to-back support & warranty along with supply of spare with appropriate response time from OEM and these Back-to-Back contracts will be shared with owner before start of defect liability period. The contractor shall be responsible for coordination with the OEM for all matters related to that equipment. The Contractor shall be responsible for meeting the overall response times and availability requirements specified in the Specification. The maintenance of the System shall be comprehensive and shall comprise of the following category of works which is further elaborated for each of the different subsystems:

a) Preventive Maintenance Activity (performance monitoring, system backup, patch management, updates, emergency response and troubleshooting)
b) Maintaining spares on a continuous basis for meeting the availability requirement.
c) OEM Back-to-back Support
    i. All the supplied systems shall be under OEM (Hardware and Software) warranty & support as per the provisions of contract along with other scope of works specified under the contract.
    ii. Contractor has to submit annually documentary evidence for the availability of OEM support for the supplied items including continuity of security patches.
    iii. Owner shall be able to login independently to OEMs (hardware and Software) portal (if available) to view support contracts and raise RMA directly with OEM if required.

7.4 Maintenance and Support Services Scope

The Contractor shall be responsible for the maintenance and support services of entire systems (Hardware and Software) supplied under the project during entire period of the Maintenance contract

Maintenance and support services shall include various scopes specified under various sections of technical specifications which inter-alia includes following without any additional cost to owner:

a) In case of failure of automatic uploading of IEM data in AMR System due to any reason, operator at AMR control center shall ensure that concerned station in-charge shall collect missing data and upload data through web application.
b) In case of any change in CT or PT ratio in any feeder due to replacement/ augmentation, the same should be incorporated in AMR software for proper recording based on the input from Generator Company/ Transmission Licensee & confirmation from RLDC.
c) OEM back-to-back support shall mean OEM back-to-back warranty and support from OEMs for all the supplied system items (Hardware and Software) under the project. OEM support shall also include all patch support (including security patches) on back-to back basis.
d) During the period of the contract if OEM discontinues or declares end of support/end-of-life, whichever is later, for any item supplied (Hardware/Software) under the contract, but the items are functional & meeting performance criteria, then these items can be maintained by either the Contractor or through back-to-back OEM/3rd party support without any additional cost to the owner. However, in case the items become either non-functional or degraded in performance during entire contract period, the same shall be replaced by the Contractor without any additional cost to the Employer. Security Solutions/Operating

System/Databases are also considered in Hardware/Software items and for Cyber Security Solutions supplied under the project shall also be made available. Replacement shall be of either same or higher configuration considering required performance specified under the contract.

7.5 Preventive Maintenance Activity

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

a) Repair / replacement of defective equipment. The Contractor shall be responsible for repair/replacement of all the hardware including consumables required for various systems.
b) Configuration of the replaced hardware and software, periodic routine checking as part of a preventive maintenance program (as described in further detail in this document) which would include checking of functionality of hardware and software.
c) Monitoring the performance of the system and doing necessary tuning for optimum performance to accommodate any changes such as the addition of new components.
d) Providing all necessary assistance to Employer/Owner as per Responsibility matrix defined in this section.
e) Auto Backup of the system at regular interval and Monitoring of all auto backup scheduled.
f) Database sizing activities including Backup and restore of the system. Any replacement or upgrade of hardware and/or software to meet the power system sizing as per table would be the responsibility of the contractor at its own cost.
g) Restoration of the systems upon its failure and to restore the functioning of the various systems at the respective Control Centres.
h) Verification of endpoint security updates
i) The contractor shall maintain register for all the activities carried out during preventive maintenance.
j) The contractor shall maintain list of inventories of all hardware and software items being supplied along with software bill of material (SBoM). The inventory shall include version/firmware number for understanding of applicable vulnerabilities from publicly disclosed vulnerabilities databases and shall take required action.
k) Physical hardware checks to ensure proper working of cooling fans etc.
l) Physical inspection to check the machines and the panels for rat droppings, lizards or other vermin.
m) Cleaning and blowing for removal of dust from Servers, Workstations and associated panels

7.6 Resource Deployment, Management & Escalation:

Contractor shall deploy qualified and well-trained human resources at AMR Control centres located in the following manner:

a) One person at each AMR Control Centre i.e. (NRPC, WRPC, SRLDC & NERPC) shall provide support for 24x7x365 days (1 no. in each shift) shall be available round the clock (in 3 shifts)

b) The manpower deployed in Control Centre should have adequate qualification i.e Minimum B.E./B.Tech in concerned field) and with adequate hands-on experience in managing system infra for similar operations.
~~c)~~ Apart from above one manpower shall be deployed at each AMR Control Centre as project coordinator. The manpower will attend office as per schedule of the respective control centre from 9:00 am to 6:00 pm. The manpower will follow the holiday list of respective control centre. In case of any urgency, the manpower will visit the control centre to resolve the issue.
d) The manpower deployed shall be from direct payroll of the Contractor and shall be an employee of the contractor.
e) Under the project scope, Contractor to ensure availability of field devices (i.e. IEM, AMR and associated equipment supplied under the project). Visit of the manpower to any substation may also be required in case of critical condition.
f) The contractor shall identify common panel of experts that will provide online support in critical conditions, if required In case of Remote operation/Online Support authorization from Employer/Owner should be taken by the contractor and contractor must complying to relevant cyber security standards for Remote operation/Online Support for resolution of the problem in the system. Visit of expert team may also be required during critical conditions.

7.7 Human Resource Management & Escalation:

a) The resource envisaged by the Employer/Owner is minimum. However, Contractor shall suitably assess the resource requirement to meet the performance requirement as stipulated in the specifications and shall deploy additional resources, if need be.
b) Contractor shall submit CVs of the proposed maintenance engineers & experts for deployment, clearly stating their qualifications, experience and competency including courses successfully completed in the relevant fields separately to the Employer/Owner for review & approval, well before deployment. The Contractor is required to replace their engineers immediately whenever the Employer/Owner on the grounds of their performance and / or behaviour requests the same during execution of duties etc.
c) The Contractor shall keep a strict check on the attendance of their engineers at respective control center to ensure their presence. The records shall be made available to the Employer on demand.
d) The Contractor shall make alternate arrangements when their shift engineers fall sick or proceed on leave, except for short duration (less than or equal to two days) during emergencies. However, the absence of their Engineers at any of the locations shall not relieve the Contractor to meet the required performance parameters stipulated under this specification.
e) The Contractor shall submit escalation procedure/ personnel contact details for reporting problems till its resolution.

7.8 Maintenance Audit

The Contractor shall perform audit of the system and Applications (preferably in the 3rd Quarter of every year) and the report shall be submitted to the Employer/Owner within fifteen (15) days.

a) Performance audit
b) Software vulnerability assessment

c) Hardware Resources Utilization

Based on the outcome of the audit, Contractor's experts may undertake necessary steps to improve the performance of the system, if applicable.

7.9 Spares Management

a) Contractor shall maintain its own inventory of requisite no. of all types of spares required for meeting the system availability requirements as per the specifications.
b) Contractor shall undertake appropriate planning for the storage of spares at strategic locations/ store depots on its own to meet the performance criteria.
c) Contractor shall submit a location wise list of spare items being maintained by them, indicating the total number of such items required to meet the performance criteria as stipulated in the specifications. However, minimum requirement list does not absolve the Contractor in meeting performance requirement under this maintenance services agreement due to non-availability of spares. Contractor shall on its own increase the spare items above the minimum list, if the situation demands so, to meet the performance parameters.
d) Contractor shall submit spares reconciliation statement every quarter to the Employer/Owner
e) All repair management related activities shall be handled through the designated Repair Management Centre and/or Technical Assistance Centre.

7.10 Preventive Maintenance, Updates & Upgrades:

The Contractor shall submit a detailed plan of Scope, schedule and formats for Preventive maintenance for Employer's/Owner's approval during detail engineering.

a) The Contractor shall do the regular monitoring of the system on 24X7 basis and shall take prompt action upon noticing any defect/fault in the system and restore it back to normal with minimal delay. This shall include organizing, coordinating, and undertaking necessary site visits for repair / replacement of faulty equipment/cards/modules etc. of supplied system by the contractor's engineers.
b) The Contractor shall rectify any errors that substantially degrades the performance of the product or materially restricts the Employer's/Owner's business.
c) The Contractor shall supply and install the new Software Upgrade Releases (both minor & major), Software Updates and/or Service Packs for system including Operating System and latest versions as generally made available by the Contractor from time to time during the entire period of this maintenance services. The updates shall be installed only after they have been duly verified and tested in the lab against crashes & vulnerabilities. The installation of new releases shall not hamper the functioning of the operational network. All software updates & upgrades shall be in the scope AMC services.
    i. "Software Update" shall mean the program improvement and rectification, provided by the Supplier in accordance with the Purchaser's malfunction report against Specification of the related Software Release or by the Supplier initiatively. It will be used to fix the bugs or provide the patches for the Software provided as per the Contract/functionalities.
    ii. "Software Upgrade" shall mean the fundamental improvement, which increases the function and/or enhances the capacity or performance based on retaining the original designed purpose of the program provided by the Supplier as to the Software Release.

7.10.1 Planned Maintenance Activities

Following is the list of minimum planned/Scheduled maintenance activities to be carried out by the Contractor:

S. No.	Activity	Description	Frequency
1	Application Server Storage Review	Application Server partitions storage to be reviewed and purging of old data to improve storage space.	Once in a Month
2	Application Data Base Review	Application Data Base performance w.r.t. table size and slow queries to be reviewed.	Once in a Month
3	Hardware resource management	Memory loading, Processor usage etc.	Quarterly
4	Firewall performance Monitoring	Monitoring the performance of firewalls installed	Weekly
5	Firewall policy monitoring	Monitoring the policy and its utilization at firewall installed at Substation and control center.	Weekly

The above list is the minimum list of schedules maintenance activities. Further maintenance activities shall be finalized during detailed engineering. The contractor shall submit the report of above activities to respective control centers.

7.10.2 Routine maintenance activities

The Contractor shall undertake the following routine maintenance activities on the network and submit the report as given below;

S. No.	Activity	Frequency
1	Performance of AMR System	Daily
2	Fault rectification	Daily
3	System/data backup	Daily
4	Incident Management Reports	Daily
5	MIS report	Monthly
6	Inventory Reconciliation	Quarterly
7	Outage Management & Planned Maintenance report	Monthly
8	User login Report	Monthly
9	System Availability Reports	Monthly
10	Audit reports	Monthly
11	Helpdesk report	Weekly

The above list is the minimum list of scheduled maintenance activities. Further maintenance activities shall be finalized during detailed engineering The contractor shall submit the report of above activities to respective control centers.

7.11 Integration of new equipment

New substation/New bays in existing Substation are likely to be added to match the growing Power system. These substations/New bays will necessitate the installation of IEMs, DCUs (as applicable). Integration of these items in the AMR System is to be done by the Contractor. It is envisaged that during the scope of the project, there shall be no requirement of upgradation of Hardware / software at the control center. The integration services to be provided by the contractor

will include the mapping of the new IEMs in Database of AMR System for onward interfacing with MDP system. Quantity mentioned in the BOQ is indicative only and actual quantity may vary and the payment shall be made as per actual quantity and Unit rate as per BPS. The contractor shall ensure that Integration of new equipment is completed within period of 15 days.

7.12 Documentation & Reports:

a) Contractor shall submit maintenance philosophy document which will be submitted for approval during detail engineering.
b) The Contractor shall submit the fortnightly, quarterly and consolidated annual Performance Reports indicating routine and specific jobs done to the concerned centers. The reports shall also include the recommendations for improvement and strengthening of the operations and management process/procedures, constraints, if any.
c) The Contractor shall submit the consolidated monthly report of incident reports to the respective Engineer-in-Charge of the state, Regional, Main and National control Center. The report shall have two sections for each incident.
    i. Faults which have not been resolved within the stipulated performance criteria limit and
    ii. Faults which have been resolved within the stipulated performance criteria limits.
d) The incident report, shall be duly signed by representative of Contractor and Employer/Owner, shall contain the following information:
    i. Fault details: Nature of fault, date & time of occurrence of the fault, time of reporting (either noticed by the Contractors' maintenance engineer or verbal/written communication from Employer/Owner), date & time of access to the equipment at site and date & time of rectification of fault.
    ii. Details of contractor's spares consumed, if any. Details of faulty item/card/module & replaced item/card/modules, source/ store/location it was sourced from etc.
    iii. Details related to analysis like identification of fault, method of rectification carried out and further course of action including repair of card etc.
    iv. Any other relevant information
    v. Recommendations for eliminating the repeat of similar faults in future.
    vi. Unauthorized login attempt report
    vii. Latest patch and software upgrade report.
e) Any other report/Document as finalized during detail engineering.

7.13 Performance Requirement

1. Definitions:

a) Service Window: "Service Window" means the service coverage hours for the system/component. In case of a service window of 24X7, the calls shall be serviced India round the clock. Critical calls (Service affecting) shall be attended on priority.
b) Reporting Month and Measurement Period:
    i. "Reporting Month" is the month in which the SLAs for the Measurement Period will be reported.
    ii. "Measurement Period" is the period of twelve calendar months ending with the last day of the month immediately preceding the Reporting Month.

c) Scheduled Hours: "Scheduled Hours" means the aggregate number of hours in the given reporting period during which the supported infrastructure elements and applications have to be available for use by the designated users.
d) Total Downtime: "Total Downtime" means, out of the Scheduled Hours, the aggregate number of hours in the reporting period during which the supported infrastructure elements and applications were unavailable for use by the designated users.
e) Planned Downtime: "Planned Downtime" means the aggregate number of hours out of the Scheduled Hours in any reporting period during which the supported infrastructure elements and applications were unavailable for use by the designated users due to preventive maintenance or upgrades.
f) Excusable Downtime: "Excusable Downtime" refers to the total downtime attributable to reasons mentioned below and shall be excluded for calculation of outage/degradation of links:
    i. Outage due to force majeure like Fire (excluding due to bad design, quality of material or poor workmanship in subject project), earthquake, riots, floods, storms, curfew, imposition of emergency etc.
    ii. Outage due to unavailability of ISTS Communication System
g) Response Time: "Response Time" refers to the time taken by the helpdesk to log and acknowledge the incident. The medium for acknowledging the incident shall be email.
h) Resolution Time: "Resolution Time" means the time taken to resolve the incident or to provide an acceptable work around for the incident.

7.14 Availability Requirements and Penalty during AMC

a) AMR system availability shall be computed on monthly basis on respective region wise i.e. NR, WR, SR & NER. Monthly Availability Report shall be put up to Employer/Owner by the Contractor with reasons for data non-availability through AMR along with the calculated penalty as per the penalty rate provided in Severity Table. The Employer/Owner shall review the same and levy the deduction on monthly basis

System	Requirement	Deduction/Penalty
Availability of 5 min Load survey data at AMR control center on Monthly basis (AMR system availability)	100% (By AMR or Manual upload)	As per Severity Level table below

Severity level: Following are the severity levels in terms of breakdown maintenance work and associated penalty to be imposed against non-compliance within stipulated time:

Severity Level	Description	Resolution time allowed When site visit not required	Resolution time allowed When site visit required	Penalty for if not resolved within allowed time on each occasion. (in INR)
Severity (Level 1A)	Both servers down/not working	< 24 hours	3 days	Penalty= (X*No of days beyond permissible) / 30

				X=0.25% of contract price OR 25% of AMC charges for the month whichever is higher.
Severity (Level 1B)	The non-availability of both the servers for minimum 1 hr upto 2 times a day shall be excluded from the calculation. Whereas, if no. of such outage exceeds than as specified above, the system shall be considered as unavailable for 6 hrs.	< 24 hours	3 days	Penalty= (X*0.25*No of days in a month for which both servers were not available for 1 hr more than 2 times in a day) / 30 X=0.25% of contract price OR 25% of AMC charges for the month whichever is higher.
Severity (Level 2)	When one server is down / not working.	< 24 hours	3 days	Penalty= (X* No of days beyond permissible) / 30 X=0.125% of contract price OR 12.5% of AMC charges for the month whichever is higher .
Severity (Level 3)	When DCUs are faulty or Problem in Ethernet Switch etc.	2 days	7 days	Penalty=(X*No of days beyond permissible) / 30 X=0.125% of monthly AMC charges for each DCU / Ethernet Switch failure during the month.
Severity (Level 4)	When data from meters are not available in the AMR	2 days	7 days	Penalty=(X*No of days beyond permissible) / 30 X=0.05% of monthly AMC charges for each meter data not available during the month.

b) Penalty for not deploying/non-availability (absence/leaves without replacement for more than three days) of manpower resources at the indicated locations shall attract penalty of Rs. 5,000/- per day.

c) If the resources are not deployed/ not available (including leaves) for more than 50% of time during the month then resource would be considered not available for entire month and shall attract penalty of Rs. 10,000/- per day.
d) Aggregated value of Maximum deduction i.e. penalty on account of various severity level shall be limited to 50% of AMC charges.

Note

Delay due to any reason not attributable to the contractor shall not be charged and decision of the owner shall be final.

a) Site visit means visit of experts from service center of contractor/OEM representatives to AMR control center or stations (as applicable)
b) Non-availability of data from Substation to AMR System due to problem in ISTS Communication link shall not be attributable to Contractor.

7.15 Responsibility Matrix

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

Legend • This indicates who has primary responsibility to perform this function.
A This indicates who will provide assistance.

Item	Task	Owner/Employer	Contractor
1A	Problem identification - Root cause analysis to determine whether fault is attributable to Hardware or Software.	----	●
1B	Resolution of problems involving third party maintainer where root cause is uncertain.	----	●
2A	Software problem resolution - Report problem and assist with problem identification.	----	●
2B	Provide/recommend corrections, temporary patches, workarounds or other fixes.	----	●
2C	Install and test corrections, temporary patches, workarounds or other fixes.	----	●
3A	Routine software support - Build and maintain database, displays and reports.	----	●
3B	Perform system back-ups.	----	●
3C	Restore or reinstall software from back-ups.	----	●
3D	Monitor system logs.	----	●
3E	Maintain system logs.	----	●
4A	Hardware problem resolution - Report problem and assist with defining problem.	----	●
4B	Troubleshoot problem to diagnose software- or hardware-related cause.	----	●
4C	Identify failed component and replace using parts from spares inventory.	----	●
4D	Restore operation of repaired/replaced equipment.	----	●
5A	Hardware spare parts - Manage local spares inventory.	----	●

Item	Task	Owner/Employer	Contractor
5B	Replenish local spares inventory.	----	●
6A	Cyber security monitoring - Patch Updates.	----	●
6B	Annual Cyber Security Audits.	●	A
6C	Implementation of Recommendations during Audit.	----	●
6D	Implementation of Monitoring and compliance manager for Critical Infrastructure Protection.	----	●
6E	Maintenance of Spares.	----	●
6F	System Reports.	----	●

7.16 Other Responsibilities of the Contractor

a) If any changes in the settings are warranted in the system for improving the system/ network performance, such changes may be initiated by the Contractor upon due intimation and approval of the Employer/Owner and such modifications shall be recorded in the incident report register.

b) The Contractor shall ensure proper insurance coverage to their employees working under this maintenance services agreement and the Employer/Owner shall not be responsible for any eventualities thereof. The Contractor shall also obtain all necessary insurances that are mandatory as per applicable local laws.

c) Contractor may use third party ('subcontractor') support only to perform maintenance activities for the equipment procured from the third party. Contractors' use of third party ('subcontractor') shall not relieve Contractor of its obligation under this contract.

d) All incident and Performance service levels will be reported and measured on quarterly basis.

7.17 Review meetings

a) Review Meetings shall be held once every quarter of the year during the contract period to review the technical, operational, quality and any other aspects of the Services delivered through the contract.

b) The review meetings shall be attended by the representative of both the Contractor and Employer/Owner. Formal notice for the meeting shall be issued at least 7 days in advance along with agenda points.

c) The meeting agenda shall inter-alia include but not limited to the following:
   i. Services and network related issues.
   ii. Status of spares
   iii. Issues related to unattended faults/ problems
   iv. Manpower issues
   v. Operational issues
   vi. Software upgradation issues.

d) Whenever any major outage occurs in any part of the network, an emergency meeting may be called, as desired by the Employer/Owner. Outage related issues in the context of cause, correction and prevention shall be discussed in the meeting.

Chapter 8 — Inspection, Testing & Operational Acceptance

8.1 General

All materials and parts of the system/sub-system to be supplied under the project shall be of current manufacture and from a supplier regularly engaged in the production of such equipment.

8.2 Quality Assurance and Quality Control Program

The Contractor shall maintain a Quality Assurance/Quality Control (QA/QC) program that provides equipment, materials and services under this specification whether manufactured, designed or performed within the Contractor's plant or at any sub-contractor source shall be controlled at all points necessary to assure conformance to contractual requirements. The program shall provide for prevention and ready detection of discrepancies and for timely and positive corrective action. The Contractor shall make objective evidence of quality conformance readily available to the Employer. Instructions and records for 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 Employer.

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

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 equipment.

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 employer

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 controlling the quality characteristics of the product.

The Quality Plan shall be mutually discussed and approved by the Employer 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 procedure 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 Contractor shall be required to submit all the Quality Assurance Documents as stipulated in the Quality Plan at the time of Employer's inspection of equipment/materials.

8.3 Scope of Employer

The Employer 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 the Employer, pursuant to the Contract, will include but not be limited to the following:

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

b) Witness or authorize his representative to witness process, 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

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

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

8.4 Inspection and Testing

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.

Documents identified in the hardware and software quality assurance plan and procedures shall be inspected to verify that the required quality assurance activities have been performed in the manufacturing process of hardware and software.

If 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) all variances have been resolved and all variance report submitted, (b) all the test records have been submitted, (c) Employer acknowledges in writing the successful completion of the test.

8.4.1 Inspection

Access to the Contractor's facilities while manufacturing and testing are taking place, and to any facility where hardware/software is being produced for Employer shall be available to Employer

representatives. The Contractor shall provide to Employer representatives sufficient facilities, equipment, and documentation necessary to complete all inspections and to verify that the equipment is being fabricated and maintained in accordance with the Specification. Inspection rights shall apply to the Contractor's facilities and to subcontractor facilities 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 labelling. 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 Employer.

8.4.2 Testing

a. 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 with 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.

During the development of test plans and test procedures for the system, emphasis shall be placed on testing each conditional logic statement, checking error conditions, and documenting the simulation techniques used. The test plans and test procedures shall be modular to allow individual test segments to be repeated as necessary.

b. Test Plan

The test plans shall describe the overall test process, including the responsibilities of individuals and the documentation of the test results. The following shall be included in the test plans:

a) Test schedule on a day-by-day basis

b) Responsibilities of test engineer and QA/QC personnel

c) Record-keeping assignments, procedures, and forms

d) Procedures for monitoring, correcting, and retesting variances

e) Procedures for controlling and documenting all changes made to the hardware and software after the start of testing

f) Block diagrams of the hardware test configuration, the external communication channels, and any test or simulation hardware.

c. Test Procedures

The test procedures shall describe the individual tests segments and the steps comprising each segment, particularly the methods and processes to be followed. The test procedures in general shall include the following items:

a) Name of function to be tested;

b) References to the functional, design, user, and any other documents describing the function;

c) List of test segments to be performed and the purpose of each test segment;

d) Set-up conditions for each test segment, including descriptions of the test equipment;

e) Descriptions, listings, and instructions for test software tools and displays if any;

f) Step-by-step descriptions of each test segment, including user actions for each test step;

g) Expected results for each test segment, including pass/fail criteria;

h) Descriptions of the techniques and scenarios to be used to simulate system field inputs and controlled equipment;

i) Copies of any certified test data to be used in lieu of testing.

d. 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.

The records shall be keyed to the test procedures. The following items shall be included in the test records:

a) Reference to appropriate test procedure

b) Date of test

c) Description of any test conditions, input data, or user actions differing from that described in the test procedure

d) Test results for each test segment including a pass/fail indication

e) Identification of Contractors's test engineer and QA/QC representative.

f) Provision for comments by test engineer and QA/QC representative

g) Copies of any variance reports generated

h) Copies of reports, display copies, and any other hardcopy generated as part of the test.

e. Test Initiation & Completion

The following conditions must be satisfied before starting any test

a) All test plans and procedures for the test shall be available.

b) All hardware and software engineering design change orders shall be incorporated into the system under test.

c) All relevant documentation including drawings, lists of deliverables, and software functional and design documents, and user manuals shall be available.

d) A complete regeneration of the software under test shall be performed immediately prior to the start of factory testing.

e) All operating system parameters, files, and configuration information shall be saved to archive media so that the AMR systems operating environment can be recreated starting with an un-initialized system. The existence and completeness of this data shall be demonstrable.

f) All database, display, and report definitions shall be saved to archive media so that the databases, displays, and reports can be recreated if necessary.

g) The image backup of all applications of AMR Systems shall be taken on the archive media so that AMR systems software can be regenerated if necessary.

h) A complete dry run of each factory test (excluding the integrated system test) shall be conducted by the contractor using the test plans and test procedures.

A test shall be deemed to be successfully completed only when:

a) All variances have been resolved

b) All test records have been documented and issued

c) QA/QC/employer acknowledges, in writing, successful completion of the test

f. Factory Acceptance Test (FAT)

The factory tests shall be conducted on test bed comprising of end to end metering solution proposed by the contractor. FAT test shall include all the equipment's (all type of Meters, communication network & AMR). Testing shall include, but not limited to the following,:

a) IEM integration with AMR System

b) Verification of all functional characteristics and requirements specified in TS

c) Performance testing of Hardware and Software

d) Integrated testing with utility application, as applicable

e) Inspection and verification of all construction, wiring, labelling, documentation and completeness of the hardware

Before the start of factory testing, Contractor shall submit the test procedure for approval of employer. The Contractor shall verify that all changes applicable to the equipment have been implemented, Type tests and Data Exchange Protocol Certificates are available (as per the sampling criteria specified by the employer). As a part of the factory tests, exploratory/contra/unstructured testing shall be performed to allow Employer representatives to verify proper operation of the equipment under conditions not specifically tested in the above structured performance test. The Contractor's test representative shall be present and the Contractor's technical staff members shall be available for consultation with Employer personnel during exploratory/contra test periods. All special test facilities used during the structured performance test shall be made available for Employer's use during exploratory/contra testing.

The development Test Bed created for the complete system testing shall be separate from the production environment and shall continue to serve the purpose of development system, for the total duration of the project

g. Factory Test Requirements

The data base displays, web based user interface displays, consumer portal and the report formats developed by the contractor shall be demonstrated and verified by the employer before factory testing.

All equipment / system shall be tested and demonstrated for performance & compliance to the standards as per the approved factory test plan. The Employer will participate in and witness these tests.

The contractor shall also carry out testing of their standard protocol and interfaces for successful integration with existing system of employer before FAT starts. The database and the report formats developed by the contractor for Control Centre shall be verified by the employer before factory testing.

The control centre redundant hardware and software architecture shall be staged and completely tested with simulated data at the Contractor's facility. The inspection clearance certificate for all hardware shall be issued only after successful completion of FAT as per specification. FAT shall be carried out at a subsystem or module level and shall consist of all the components of the system being supplied to the extent possible.

The employer shall witness all tests and will not accept un-witnessed test results. Each of the factory tests described below (i.e. Routine & Acceptance Test of IEMs), the hardware integration test, the functional performance test, and the integrated system test, unstructured tests) shall be carried out under factory test.

h. Sample Routine & Acceptance Tests for IEM

These tests for IEM are in addition to the Type Test requirements specified and the Routine and Acceptance tests that the Contractor will carry out as a part of their FAT procedure.

The sample Routine and Acceptance tests as per IS 14697 shall be performed in a third-party **NABL** accredited laboratory. The employer shall have the authority of selecting the samples (in accordance with IS 14697) for carrying out the Routine and Acceptance Tests. The contractor shall be obliged to undertake these tests at their own cost. The sampling criteria and conformity requirement shall follow IS 14697 as the case may be.

The contractor shall be responsible for packing, handing over the material to the respective labs and ensuring transportation of the material directly from the manufacturer's location to the Labs for testing and delivering the material to site after successful test results are obtained. The contractor shall be obliged to undertake all expenditures that shall be incurred towards packing, transport, inspection, testing charges etc.

The lot wise testing shall be as per following methodology:

i. Sample Routine & Acceptance Tests shall mandatorily be carried out on each lot as per standard policy of employer

ii. In addition to the above, the Employer reserves the right to carry out accuracy tests, in line with the above guidelines, in their own Meter testing Laboratory for each lot.

i. Hardware Integration test

The hardware integration test shall confirm that the computer hardware conforms to this Specification and the Contractor-supplied hardware documentation. The hardware integration test shall be performed when the computer hardware has been installed in the Contractor's factory. The operation of each item shall be verified as an integral part of the system. Applicable hardware diagnostics shall be used to verify that each hardware component is completely operational and assembled into a configuration capable of supporting software integration and factory testing of the system. Equipment expansion capability shall also be verified during the hardware integration test.

j. Functional Performance Test

The functional performance test shall verify all features specified in respective technical specifications of equipment/ systems & software using selected communication paths**.** During the Functional Performance tests at least 20 IEMs & 4 DCUs shall relate to each central system and the remaining Field devices shall be simulated in the factory test environment. The data exchange between central systems shall also be simulated in the factory test environment. As a minimum, the following items shall be included in the functional performance test:

a. Inspection of all equipment for conformance to drawings/document and satisfactory construction and appearance

b. Testing of the proper functioning of all software, including test cases with normal and exception user-entered inputs and responses

c. Verification that ultimate expansion requirements are met

d. Input power supply failure to device, hardware to verify system behavior.

e. Demonstration of all features of software functionalities as per Technical Specification.

f. Verification of User Interface displays, functions, including random tests to verify correct database linkages and reports

g. Demonstration of all features of the database, display, and report generators and all other software maintenance features. These shall include but not be limited to functional features

h. Demonstration of the software utilities, libraries, and development tools, as applicable

i. Verification that the computer system meets or exceeds performance requirements

j. Verification of the accuracy of hardware and software documentation via random tests

k. Sample check of meter calibration accuracy and testing of spare parts.

The details of tests and test procedures shall be finalized during detailed Engineering. Contractor shall submit the documents for tests and test procedures for approval of Employer.

k. Integrated System Test (to be carried out with first Lot only)

Integrated system test shall be performed after successful completion of functional performance test. During the integrated system test, all functions shall run concurrently and all Contractor supplied equipment shall operate for a continuous 100-hour period. This minimum level of activity during this period shall be as per the discretion of employer. These other activities may include, but shall not be limited to, database, display, and report modifications, software development activities, configuration changes (including user-commanded server and device failovers), and the execution of any function described in this Specification.

The integrated system test shall assure employer that the web services/computer system at POWERGRID/Utility is free of improper interactions between software and Hardware while the system is operating as an integrated unit. In case during the 100 hours period testing uncommented functional restart or device fail occurs the test shall be extended by 24 hours each time such a fail-over occurs. Further the test shall not be conducted with the failed device.

l. Unstructured Test

Employer representative can carry out unstructured test not specified in the test procedure. Minimum 25% of the actual time shall be kept reserved for unstructured test. Contractor's representative shall carry out such test at employer's discretion but after the completion of functional test. All simulation software, test cases, and other test facilities used during the structured portions of the factory tests shall be available for use during unstructured testing

8.5 Testing requirements of AMR system

All equipment, materials and software for AMR System shall be subject to both Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT). The purpose of Acceptance Testing is to determine compliance to this specification in every respect for the delivered and installed system

A. Acceptance Test Plan and Procedures

The Vendor shall develop and document proposed Test Procedures and Test Plans for Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) of the delivered and commissioned system and its components. The final Test Procedures and Test Plans shall be subject to review and approval prior to testing.

The ATP shall include, but not be limited to, functional tests that demonstrate compliance of the functional, performance, software, hardware, interface, and operational aspects of the complete system.

B. Factory Acceptance Test (FAT)

The Vendor shall perform a preliminary FAT (Pre-FAT) prior to the FAT. The pre-FAT shall be a complete dry run of the FAT, following the test plans and procedures. The intent is for the Vendor to detect and correct most design, integration, database, display, and performance problems prior to the FAT. The representatives of Employer shall have the right to witness all or parts of pre-FAT for which vendor shall intimate the schedule to Employer sufficiently in advance.

Test results (including documentations and certifications) for tests conducted by Vendor or third parties that are not included in the FAT test plan and procedures shall be furnished to Employer prior to FAT for review and verification. Vendor and/or third parties conducted tests deemed inadequate shall be repeated for acceptance of Employer.

Vendor's project manager shall sign off each test of Pre-FAT. The completed test results shall be sent to Employer for review before their representative's visit to the Vendor facilities for the FAT. All tests shall be conducted using the contract-specified databases unless Employer authorizes the Vendor to use a test database.

The FAT shall be conducted according to the FAT Test Plan and Test Procedure documents approved by Employer shall cover, as a minimum:

- **Visual Inspection –** To verify that the system to be delivered has all required components and is properly configured. Visual inspection shall verify acceptable workmanship and that all equipment, including cables and connectors, are appropriately labelled
- **Hardware Diagnostic Test –** Individual tests of all system hardware. These tests shall consist of running standard hardware diagnostic programs, plus all special diagnostic programs used by the Vendor.
- **Communications and Interfacing Test –** Verify that all interconnected system components, such as data acquisition, control, monitoring, and data management functions are operating properly when correctly connected.

- **Functionality verification –** Verify that all system functions are working normally as set forth in the contract.
- **Performance Testing –** Verify that the system throughput, timing and response time requirements are satisfied. Tests shall include verification of:
    - Data exchange times between IEM and DCU and DCU to AMR system
    - User Interface function response time

  This performance requirement shall be met under the maximum number of input DCUs and maximum number of IEMs as specified during detailed engineering.

- **Security Testing –** Verify that the software meets security requirements at delivery and other aspects of secure operation and system access including:
    - Communication error detection capabilities
    - Correct operation of system configuration, control, maintenance, and management procedures
    - Safe system recovery with no erroneous data or control operation generation after system restarts
    - Protection against unauthorized access to the system and control functions
    - Compliance to CERT-In standard & CEA (Cyber security in power sector) Regulations'2026
- **Environmental Testing –** Verify that
    - All system functions shall operate correctly over the specified temperature range
    - The accuracy of the inputs and outputs remain valid over the specified temperature range.

  The test schedule shall allow sufficient time for verification and/or additional unstructured testing by the Employer's representative, who shall be able to schedule unstructured testing at any time, including during structured tests.

8.6 Dispatch of Material

The Material Inspection Clearance Certificate (MICC) for all hardware shall be issued by Employer only after successful completion of FAT as per specification. For this Contractor is obliged to submit a comprehensive FAT clearance report to the Employer. All Equipment Suppliers/OEMs to the project shall make use of categorised Interim Inspection Reports (CIP Clearance) from Employer to ship materials to site after completion of FAT. CIP shall be issued by the Employer subject to successful FAT report. Categorised Interim Inspection Report with the lowest category would mean a complete failure of FAT and hence rejection of material. A category between the lowest and the highest, shall mean pending actionable points of minor nature, but material deemed fit for dispatch to site. The category of CIP shall be issued by the Employer. In case where CIP with the highest category (with no pending actionable points in FAT), the Employer shall issue a Material Inspection Clearance Certificate (MICC).

8.7 Site Acceptance Test

Once the contractor finalizes the SAT schedule, shall invite the employer to witness the tests as per their convenience. SAT will be carried out with field devices (IEMs & DCUs etc) in lots

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 SAT shall exhibit generally all functions of the equipment All variances must be corrected prior to the start of the SAT.

The contractor shall list of final tests to be carried out in the field shall be listed in the site-testing document.

After the equipment has been installed, the Contractor shall check the performance of the equipment in site field locations. All data services shall be integrated with the field equipment and peripheral devices, all inputs and outputs interfaces installed & integrated with relevant software all test readings recorded in accordance with the SAT procedures. Contractor to submit consolidated SAT document for approval of employer.

After the Site Acceptance Test (SAT) of each AMR Control Centre at respective RLDC, a 100-hour availability test shall be conducted on all supplied systems in an integrated and simultaneous manner under normal day-to-day operating conditions. The test shall verify the reliability and integrity of the database, report and all communication interfaces and, under these conditions, verify system availability for 99.9%. Further each server and device if applicable shall meet a minimum availability of 98% individually. In case of field devices, if applicable, downtime of individual such devices are to be excluded from system availability calculations, however, minimum 50% of field devices shall be reporting for test to continue.

8.8 Contractor's Maintenance Responsibility till Operational Acceptance

During this period, the Contractor shall make available resident Project Manager, software & data services specialists, who shall be available upon notification by the Employer about any problem(s) that may exist. The contractor's specialists shall be required to respond to the Employer notification in line with the provisions of technical specifications. The contractor shall replace or repair all defective parts and shall have prime responsibility for keeping the system operational.

8.9 Type Testing & Data Exchange Protocol Testing

“Type Tests" shall be defined as those tests which are to be carried out to prove the design, process of manufacture and general conformity of the materials to this Specification and BIS standards. The Data Exchange Protocol Tests are defined as those tests which establish compliance with DLMS/COSEM application layer Type Testing the Data Exchange Protocol Testing shall comply with the following:

(a) The Contractor shall submit copies of test reports and certificates for all of the Type Tests that are specified in the specifications and that have previously been performed (before contract award). These certificates may be accepted by the Employer only if they apply to materials and equipment that are essentially identical to those due to be delivered under the Contract and only if test procedures and parameter values are identical to those specified in these specifications carried out at nationally accredited labs and valid as per relevant specification of the equipment.

(b) Type Tests shall be performed for all equipment types for which certification is not provided as required in (a) above, or if it is determined by the Employer that the certification provided is not acceptable. If any of the type tests are required to be carried out, the same shall be carried out by the Contractor after informing to employer at its own expenses. The charges for carrying out that test(s) shall not be payable by the Employer.

(c) Type Tests and Data Exchange protocol tests shall be certified or performed by nationally third party NABL accredited or equivalent laboratories using material and equipment data sheets and test procedures that have been approved by the Employer. The test procedures shall be formatted as in the specifications and shall include a complete list of the applicable reference standards and submitted for Employer approval at least four (4) weeks before

commencement of test(s). The Contractor shall provide the Employer at least 15 days written notice of the planned commencement of each type test.

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

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

(f) In case of failure during any type test, the Contractor shall modify the equipment and shall repeat the type tests on that equipment at its own expenses. The type tests to be repeated shall be decided by the employer depending upon the severity of the failed test.

(g) Documentation for all factory, field, and availability tests that apply to the AMR system shall be provided in accordance with the requirements defined in this section of specification.

8.10 Operational Acceptance

1. Establishment of AMR Control Centre
2. Installation, Commissioning & Integration of IEMs along with AMR system including its integration with MDP / Certification of RLDC
3. Initial third-party Cyber Security Audit Report

Chapter 9 — Documents, Drawings and Deliverables

9.1 General Documentation Requirements

All documentation for the IEM, DCU, AMR and MDP systems shall be supplied in hard copy as well as computer-readable soft version, and shall be complete, accurate and kept current through the guarantee/AMC period. Documentation obligations are summarized below by system component.

9.2 Design Documents

Prior to manufacture/development, the Contractor shall submit design documents covering, at minimum: system overview and complete network schematics; functional/flow-chart diagrams; functional/technical details of major components; system configuration and design documentation; the applicable testing procedures (Type/Routine, FAT, SAT); and the Cyber Security policy per CERT-In guidelines together with a compliance report against CERT-In standards and the CEA Cyber Security Regulations'2026.

9.3 Software Requirement Specification (SRS)

Following approval of the design document, a Software Requirement Specification (SRS) document for the AMR/DCU application software shall be prepared and submitted for approval. Software shall be designed strictly to the approved SRS.

9.4 User Manuals and Training Documentation

- User manuals for the complete AMR system, including the DCU.
- Operation & Maintenance manuals for the AMR system, including the DCU.
- A central-site user manual covering all user instructions, block diagrams and user screens necessary as a self-contained reference for operating the complete metering system.
- Comprehensive product, installation and O&M manuals for the DCU, together with video tutorials for common issues, uploaded and made available on the AMR server, accessible to all connected substations via a web application link.

9.5 Testing Documents

Testing documents shall be prepared and submitted per the Testing Requirements of Section 12, covering Acceptance Test Plans and Procedures, FAT reports, SAT reports, Commissioning Test reports, and cyber-security audit reports.

9.6 Software and Licence Documentation

The Contractor shall furnish comprehensive documentation for all software supplied, deployed, configured, or used as part of the solution. The documentation shall, at a minimum, identify the software name, version/release number (as applicable on the date of FAT/SAT), manufacturer/developer, purpose of use, license type (third-party commercial, proprietary, open-source, or freeware), and license validity period (perpetual, subscription-based, term-based, or otherwise).

A separate software license register shall be provided identifying all software components that require periodic license renewal, annual maintenance, subscription, security updates, version upgrades, or ongoing vendor support.

The Contractor shall ensure that all software licenses required for satisfactory operation of the system during the Contract, warranty, and support period are valid and legally obtained.

9.7 As-Built and Historical Documentation

The Contractor shall furnish as-built drawings and configuration records reflecting the system as finally commissioned, together with historical-record extracts demonstrating traceability of Master File, formula and CT/PT-ratio changes over time.

9.8 Certificates

- Copies of IEM type-test certificates
- Copies of IEM and AMR warranty/guarantee certificates
- System-availability certificates accompanying each monthly AMC bill

9.9 Packaging & Protection

All the materials shall be suitably protected, coated, covered or boxed and crated to prevent damage or deterioration during transit, handling and storage at Site till the time of installation. The Contractor shall be responsible for any loss or damage during transportation, handling and storage due to improper packing. Any demurrage, wharfage and other such charges claimed by the transporters, railways etc. shall be to the account of the Contractor.

Chapter 10 — Project Management & Implementation Plan

10.1 Introduction

This section describes the project management & implementation plan for the project.

10.2 Project Management

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

Work area is spread across substations of various utilities. Coordinator shall be nominated by respective utility who shall be responsible for work under their jurisdiction (arranging of outage / installation clearance etc.)

Minimum Qualifications of the project manager shall be B.E. /B. Tech in ECE/CS Engineering/MCA. PM should possess at least 10 years of experience in similar works.

10.3 Project Schedule

Time is essence of the contract. Based upon this the contractor shall submit a preliminary project implementation schedule along with the bid. The detail project implementation schedule shall be submitted by the Contractor after award for Employer's/Owner's approval, which shall include at least the following activities:

a) Site Survey

b) Documents, DRS, Drawing submission and approval

c) Hardware and software purchases, development/manufacturing and integration

d) Factory Acceptance Testing commencement and completion.

e) Dispatch Schedule

f) Receipt, Storage, Installation & Field update schedule

g) Integration of all supplied subsystems

h) Testing at Site/control Center for integrating with existing system

i) Training schedule

j) Commissioning of entire system, SAT of the system -commencement and completion

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

10.4 Site Survey and Detailed Engineering

On commencement of contract, the contractor shall collect necessary site details by visiting each site. Detailed engineering shall finalize: exact IEM/DCU counts per region and per station; the

number of Ethernet switches per station; DC auxiliary voltage at each station; SLDC-specific meter lists for the 1-minute MW viewer; the CTUIL feed data set, format and refresh interval; and whether the AMR system is hosted at the RPC or the RLDC. Availability of firewall at substation is to be included in the survey report.

10.5 Progress Report

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

10.6 Transmittals

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

10.7 Review Meetings

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

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

10.8 Outage Coordination

Installation of IEMs at interface points may require shutdown of transmission elements. All such shutdowns shall be coordinated through the outage-coordination procedure approved by the Regional Outage Coordination Committee (OCC) forum. Necessary coordination for the outage shall be done by coordinator of respective utility in whose substation premises the IEM is to be installed. Contractor needs to coordinate with the respective utility well in advance for smooth execution of work.

10.9 Manpower resources

Deployment of qualified and experienced project personnel, including Project Manager, Design Engineer, Communication Engineer, Cybersecurity Specialist, Site Manager, Commissioning Engineers (capable of working under live switchyard condition) and other experts necessary for successful implementation and operation of the project. The Contractor shall communicate details of such personnel to the Employer and maintain an adequate project team to complete the project.

Section 11 — Training and Knowledge Transfer

11.1 Training Philosophy

Training under this Project is structured in three tiers, corresponding to the three principal system components — IEM, AMR (including DCU), and MDP — so that Owner/Employer/RLDC personnel are equipped, at the appropriate level of depth, to operate, configure and troubleshoot the equipment they are responsible for, both immediately after commissioning and on an ongoing basis through informal knowledge transfer during the AMC period.

11.2 IEM Training

A hands-on training program shall be provided for Employer/Owner personnel, covering:

- Features of IEM & Communication Interface.
- Installation of software in local PC/Laptop.
- Data downloading from IEM.
- Data uploading through web interface.
- Time synchronization through dedicated GPS, Time correction through software.

System Diagnostics Minimum duration of training program is two Hours. Comprehensive documentation including product manual, Installation manual, O&M manual should be provided to all participants. Procedure for data downloading from Meter to Local PC and video tutorials to attend minor issues shall also be provided to each site.

11.3 AMR System Training

Training program for system users shall include but not restricted to the following:

- System overview including system functionalities and features.
- System configuration and operations oriented training.
- System alarms handling.
- Local/Remote configuration procedures.
- Engineering oriented training for development/testing.
- Minimum training including hands-on for a group of system users shall be 12 hours (6 hours x 2 days).

11.4 Software Support Team Training

Training for the software support team shall cover system overview (including design and as-built configuration), system software maintenance, and system diagnostics/troubleshooting, comprising a minimum of eighteen (18) hours (6 hours × 3 days) for a team comprising representatives from various stakeholders.

The bidder shall prepare and submit, for review and approval at the start of deployment, a description of the proposed training programmes, including course content and technical level of instruction,

11.5 Knowledge-Transfer Documentation

All training shall be backed by durable documentation — product manuals, installation manuals, O&M manuals, and video tutorials for common issues — hosted on the AMR server and accessible to all connected substations through a web application link, so that knowledge transfer is not solely dependent on personnel continuity at either the Contractor or the Owner/Employer side.

Annexure A — Glossary of Terms and Abbreviations

The following glossary consolidates the abbreviations and defined terms used throughout this Project Document, for ease of reference by all stakeholders — Employer, Owner, Contractor, RLDC/NLDC, SLDC and RPC personnel.

Abbreviation	Definition
ABT	Availability Based Tariff
ATP	Acceptance Test Plan
AMC	Annual Maintenance Contract
AMR	Automatic Meter Reading
BOM	Bill of Materials
CEA	Central Electricity Authority
CERC	Central Electricity Regulatory Commission
CERT-In	Indian Computer Emergency Response Team
CMRI	Common Meter Reading Instrument
C&R	Control & Relay (panel)
CTU	Central Transmission Utility
DCD	Data Collection Device
DCU	Data Concentrator Unit
DMZ	Demilitarized Zone (network security)
DSM	Deviation Settlement Mechanism
EA	Energy Accounting
EHV	Extra High Voltage
FAT	Factory Acceptance Test
FIFO	First-In-First-Out (data buffering)
FOTE	Fibre Optic Transmission Equipment
GPRS	General Packet Radio Service
GPS	Global Positioning System

Abbreviation	Definition
GSM	Global System for Mobile Communications
GTP	Guaranteed Technical Particulars
HHU	Handheld Unit
HMI	Human-Machine Interface
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEGC	Indian Electricity Grid Code
IEM	Interface Energy Meter
IP	Ingress Protection (rating) / Internet Protocol (context-dependent)
IS	Indian Standard
ISO	International Organization for Standardization
ISTS	Inter State Transmission System
LAN	Local Area Network
LDC	Load Despatch Centre
MDP	Meter Data Processing
MoP	Ministry of Power
NABL	National Accreditation Board for Testing and Calibration Laboratories
NCIIPC	National Critical Information Infrastructure Protection Centre
NLDC	National Load Despatch Centre
NMS	Network Management System
NPC	National Power Committee (CEA Division)
OEM	Original Equipment Manufacturer
O&M	Operation & Maintenance
PCB	Printed Circuit Board
PGCIL	Power Grid Corporation of India Limited

Abbreviation	Definition
RDBMS	Relational Database Management System
REA	Regional Energy Accounting
RLDC	Regional Load Despatch Centre
RMS	Root Mean Square
RPC	Regional Power Committee
SAMAST	Scheduling, Accounting, Metering and Settlement of Transactions in Electricity (Report)
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SEM	Special Energy Meter
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SLDC	State Load Despatch Centre
SNTP	Simple Network Time Protocol
SOC	Security Operations Centre
SPOC	Single Point of Contact
SRS	Software Requirements Specification
SSH	Secure Shell (protocol)
SSL	Secure Sockets Layer
TCC	Technical Coordination Committee
TOC	Taking Over Certificate
ULDC	Unified Load Despatch and Communication (network)
VAPT	Vulnerability Assessment and Penetration Testing
VPN	Virtual Private Network
WAN	Wide Area Network
DLMS	Device Language Message Specification (metering protocol)

Abbreviation	Definition
COSEM	Companion Specification for Energy Metering
VAR	Volt-Ampere Reactive (instantaneous reactive power)
VARh / VArh	Volt-Ampere Reactive hour (reactive energy)
Wh	Watt-hour (active energy)
MW	Megawatt
MWh	Megawatt-hour
MVAr	Megavolt-Ampere Reactive
kV	Kilovolt
Vref	Reference voltage
Iref	Reference current
CT	Current Transformer
PT / VT	Potential Transformer / Voltage Transformer

Annexure B — Sample Forms

The following sample forms shall be used for project execution, quality and change control. Blank templates shall be reproduced and completed as required at each occurrence.

B.1 Weekly AMR Availability Report Form

Field	Detail
Reporting week (from–to)	
RLDC/RPC	
AMR system availability (%)	
5-min load-survey data availability (%)	
Instances of data non-availability (count)	
Reasons for non-availability	
Severity level(s) invoked	
Calculated penalty (if any)	
Prepared by (Contractor)	
Reviewed by (Owner)	

Annexure-C Model Clauses - CEA 2026 guidelines on Cyber Security in Power Sector

1. **Regulations and Statutory Guidelines**

   The Contractor shall provide the System compliant with the **Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026.** The contractor shall follow and ensure compliance with all the cyber security-related statutory regulations and guidelines, directives and advisories issued by statutory authorities such as CSIRT-Power, CERT-In, NCIIPC, CEA throughout the contract period. The System shall be designed to also comply with NCIIPC guidelines for Critical Infrastructure Protection, ISO 27001, ISO 27019 and IS 16335 standards as well as additional requirements specified in this technical specification. Where implementation of these regulations/guidelines necessitates procurement of additional third-party hardware, software licenses, or security appliances not included in the original scope, such items shall be provided by the Employer/Owner. The Contractor shall, however, be responsible for integration, configuration, testing, and implementation support thereof.

2. **Isolation of OT System**

   Physical isolation of Operational Technology system from Internet as well as Information Technology system shall be ensured. Any exchange of approved data between IT and OT networks shall be permitted only through separate communication channels and dedicated unidirectional gateways, with prior approval of the competent authority. Data flow from IT to OT and from OT to IT shall be established in accordance with applicable cyber security regulations and approved system architecture.

   The reference time source selected for Operational Technology system shall be, either terrestrial or India specific satellite based and independent of internet.

3. **Patch Management**

   Patch Management system shall be provided by contractor for all the systems and devices supplied under the project. Digitally signed or validated and authenticated, security patches and updates for all systems as well as components supplied under the project shall be made available throughout contract period or useful life of such systems, whichever is later. Details of patch management has been specified at **Appendix-A**.

4. **Logs requirements**

   The Logs of the supplied system and device including applications, network activities shall be maintained for at least 180 days. The contractor shall ensure that the logs associated with an incident including logs pertaining to one hundred and eighty days prior and post to such incident are available for at least three hundred and sixty-five days from occurrence of such incident.

5. **Backup policy and requirements**

   Backup policy shall be implemented to ensure that online or offline backup data or both, as applicable, of all critical systems is up to date, but not older than a month, and retained in a separate and safe environment for the period as specified in the data retention policy. Contractor shall ensure that at least last two working data backups are available.

   Backup architecture shall include immutable or offline backup capability and periodic restoration testing to demonstrate recovery from ransomware incidents.

Recovery and Restoration

The Vendor shall provide documented and periodically tested recovery procedures and disaster recovery plans for all supplied systems to enable restoration from cyber incidents and cyber crisis situations.

1. **Cyber Security System**

   Cyber Security system comprising of various modules as envisaged in the specification shall be supplied by the Contractor for the cyber security requirements envisaged in the specification. These components are identified in Bill of Quantities for of the projects such as Firewalls with NIPS, Routers, Switches, Data Diode, End point security including Antivirus, HIPS, SIEM, Patch Management **<as applicable>**

2. **SOPs pertaining to Cyber Security System of Supplied Systems**

   The Contractor, in association and consultation with the Employer, shall develop, submit, and maintain Standard Operating Procedures (SOPs) covering all relevant cyber security aspects of the supplied Operational Technology (OT) systems. The Contractor shall prepare, at a minimum, the following SOPs:

   - User Access and Password Management
   - Patch and Security Update Management
   - Backup, Restoration and Recovery Mechanism

3. **Network Segmentation**

   Network segmentation shall be followed as per industry's best security practices. It shall include at least the following:

   - Separate VLAN and zones should be created for different servers, network devices as per functional requirements in consultation with Employer/ Owner.
   - Network Zoning shall be implemented as per the proposed architecture given in **<Insert relevant Appendix>**. However, the Contractor may suggest other methods of network architecture for enhanced security of the System.
   - Network architecture shall be designed in such a way that Servers/ systems shall be placed in separate VLANs, thereby providing micro-segmentation of the network on the same switch. Any traffic flow from server to server or server to client/console must pass through firewalls except for the servers proposed in clusters, if any.
   - The contractor shall ensure that procured product has appropriate security, network and segregation provisions to support and enable a 'defence-in-depth' approach to the System security. The contractor shall recommend guidance on the design and configuration of network security zones within the procured product. The contractor shall provide information on all communications (e.g., protocols) required between network security zones, whether inbound or outbound, and identify each network component of the procured product initiating communication The contractor shall verify and document that disconnection points are established between the network security zones and provide the methods to isolate the zones to continue limited operations.

4. Asset Register

Asset register shall be maintained by contractor, recording the details of all critical systems along with the requisite details including its configuration, hardware, software, network architecture depicting data flows and communication protocols used in the project.

5. System Hardening Policy

All the Hardware, Operating Systems (OS) and Application software shall be hardened based on OEM recommendations and industry standards. Contractor shall provide hardening checklists for all supplied systems in consultation with employer for incorporation of employer's policies during detail engineering. A minimum cyber security and system hardening policy to be followed in supplied system is attached at **Appendix-B**. List of ports and services enabled in each hardware device must be maintained and shared after SAT of the System.

Policy implementation check must be conducted periodically (quarterly) by the contractor and report to be submitted to owner.

6. Cyber Security Audits

The Employer shall engage CERT-In empanelled auditors for conducting Cyber Security Audits, Vulnerability Assessment and Penetration Testing (VAPT), configuration reviews, and compliance assessments during Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT), and throughout the Defect Liability Period and Maintenance Period.

The supplied system is also subjected to Audit by Statutory auditors, internal auditors, or any other authorized third-party agency for conducting cyber security audits. The Contractor shall extend all necessary support, assistance, documentation, system access, test environment access, and technical cooperation required for completion of such audits.

7. Implementation of Audit Recommendations

The Contractor shall implement all applicable observations, recommendations, corrective actions, mitigations, patches, updates, configuration modifications, and remedial measures arising from such audits within timelines mutually agreed upon with the Employer based on the criticality and operational requirements of the system.

Critical and High-risk vulnerabilities identified during cyber security audits shall be remediated within one month and Medium/Low vulnerabilities within three months unless compensating controls approved by Employer are implemented.

The Contractor shall submit a compliance report and closure status against each audit observation/recommendation within the stipulated timeframe. Failure to submit the required compliance report or failure to address agreed audit findings shall constitute a Severity-2 non-compliance under the Contract.

All software updates, security patches, firmware upgrades, configuration changes, and modifications required to address vulnerabilities or audit observations in the products, systems, applications, and services supplied under the Contract shall be carried out by the Contractor at no additional cost to the Employer.

Where implementation of an audit recommendation necessitates procurement of additional third-party hardware, software licenses, or security appliances not included in the original scope, such items shall be provided by the Employer. The Contractor shall, however, be responsible for integration, configuration, testing, and implementation support thereof.

8. Vulnerability Disclosure and Management

The Contractor shall maintain an effective vulnerability management process and provide the Employer with details of all identified vulnerabilities affecting the supplied products, systems, firmware, operating systems, applications, and associated components, including CVE ID, CVSS Base Score, Temporal Score, Environmental Score, Impact assessment, Available patches or mitigation measures.

The Contractor shall also disclose vulnerabilities identified internally by the OEM/Contractor, including vulnerabilities not yet publicly disclosed, to the extent permitted by applicable confidentiality, legal, and responsible disclosure requirements.

The Contractor shall promptly assess, mitigate, and close vulnerabilities reported by CERT-In, NCIIPC, CSIRT-Power, Other Government agencies, OEM security advisories, Audit agencies engaged by the Employer. The Contractor shall provide the Employer with details of the OEM's official vulnerability disclosure and security advisory channels.

A formal structured process to report vulnerabilities in the products and services should be established. Further, the vendor shall furnish such vulnerabilities to the Computer Security Incident Response Team - Power, through its vulnerability disclosure and management program.

Remediation timelines shall be based on vulnerability severity, exploitability, operational risk, and applicable regulatory requirements.

9. Components without CVE/CVSS Publication

The Contractor shall provide and periodically update a list of software, firmware, operating systems, libraries, and components supplied under the Contract for which CVE identifiers and/or CVSS scores are not published by the OEM or are otherwise unavailable.

The Vendor shall provide digitally signed or otherwise authenticated security patches, firmware updates, and software updates for all supplied products throughout the contract period or useful life of the system, whichever is later.

For such components, the Contractor shall perform its own risk assessment and submit suitable compensating controls, mitigation measures, and recommended security practices for approval by the Employer.

10. Baseline Configuration Management

The Contractor shall establish, document, and maintain approved baseline configurations for all cybersecurity-relevant hardware, software, operating systems, applications, network devices, security appliances, and system components supplied under the Contract.

The baseline configuration documents shall be reviewed at least annually and shall be made available for verification during periodic audits conducted by the Employer or its designated auditors.

11. Security Incident and Vulnerability Notification

The Contractor shall promptly notify the Employer of any cybersecurity vulnerability, security advisory, exploit, compromise, malware incident, security breach, or cyber incident affecting products, services, software, firmware, or systems supplied under this Contract within six hours of detection and provide detailed RCA and corrective action report.

Such notification shall be made in accordance with applicable Government of India regulations, CERT-In directions, sectoral cybersecurity guidelines, and timelines prescribed by the Employer. The notification shall include impact assessment, mitigation measures, workaround recommendations, and remediation timelines.

12. Cybersecurity Point of Contact

The Contractor shall nominate and maintain throughout the Contract period one or more qualified cybersecurity coordinators as single points of contact for vulnerability management, incident response, audit coordination, patch management, compliance reporting, and cybersecurity-related communications. The Contractor shall provide and keep updated the names, designations, email addresses, and contact numbers of such personnel.

13. Third-Party Components

The Vendor shall provide documentation detailing all security requirements, dependencies, patches, updates, and integration processes relating to any third-party components included in the supplied solution.

14. End-of-Life/Support Notification

The Vendor shall notify the Purchaser of the End-of-Support (EOS) and End-of-Life (EOL) status of all supplied hardware, software, firmware, and third-party components, along with recommended replacement or migration options.

15. Bill of Materials (BOM)

The Vendor shall provide and maintain an updated Software/Hardware Bill of Materials (SBOM/HBOM), including firmware and third-party components, in accordance with applicable CERT-In guidelines. A sample format with minimum requirement to be filled and supplied by contractor is attached at **Appendix-C.**

16. Declarations and Undertakings

The Contractor shall duly fill, sign, and submit all Declarations and Undertakings in the format prescribed at Appendix**-D**. The **Non-Disclosure Agreement (NDA)** shall be executed on the requisite **Stamp Paper/e-Stamp Paper** and submitted to the Employer.

17. Third-Party Service Providers

a. If the Contractor engages any third-party service providers or subcontractors to perform services involving the handling of POWERGRID's data and information, the

Contractor shall ensure that such third parties comply with the same security requirements and obligations as set forth in this Agreement.

b. The Contractor shall conduct due diligence on any third-party service providers or subcontractors to assess their security practices, certifications, and compliance with relevant standards and regulations.

c. The Contractor shall remain fully responsible and liable for the acts and omissions of its third-party service providers or subcontractors concerning the security and protection of POWERGRID's data and information.

18. Security Awareness and Training

a. The Contractor shall provide regular security awareness and training programs to all personnel involved in the handling of POWERGRID's data and information, covering topics such as data protection, incident response, secure handling and disposal procedures, and relevant security policies and procedures.

b. Personnel deployed for operation and maintenance of critical systems shall undergo power-sector specific cybersecurity training as mandated by applicable regulations.

c. The Contractor shall maintain detailed records of security awareness and training activities, including attendance logs, training materials, and assessments, and make such records available to POWERGRID upon request for auditing and monitoring purposes.

19. Personnel Security

a. The Contractor shall conduct background checks, including criminal record checks and employment verification, on all personnel who will have access to POWERGRID's data and information, in accordance with applicable laws and regulations.

b. The Contractor shall ensure that all personnel who have access to POWERGRID's data and information receive regular security awareness training, covering topics such as data protection, handling of sensitive information, and incident reporting procedures.

c. The Contractor shall ensure that all personnel who have access to POWERGRID's data and information are bound by appropriate confidentiality agreements and are aware of their obligations to protect the confidentiality, integrity, and availability of such data and information.

20. Secure Development and Deployment Practices

a. The Contractor shall follow secure software development life cycle (SDLC) practices, including but not limited to requirements analysis, secure design, secure coding, code reviews, testing, and secure deployment processes.

b. The Contractor shall implement secure configuration management practices, including version control, change management, and separation of environments (development, testing, and production).

c. The Contractor shall maintain detailed documentation of the software development and deployment processes, including security controls, configurations, and changes made throughout the SDLC.

21. Encryption and Secure Communications

a. The Contractor shall use industry-standard encryption protocols and algorithms, such as [specify encryption standards, e.g., AES-256, TLS 1.2, or higher] for transmitting and storing POWERGRID's data and information.

b. The Contractor shall implement secure communication channels, such as secure file transfer protocols (SFTP) or virtual private networks (VPNs), for the exchange of sensitive data and information with POWERGRID.

c. The Contractor shall maintain and regularly update digital certificates, encryption keys, and other cryptographic materials used for securing communications and data.

22. Change Management Requirement

Contractor shall maintain documented change management procedures for all software, firmware, security patches, configuration changes and cyber security updates with version control, rollback capability and approval records.

23. Information Security Practices

a. The Contractor shall implement and maintain an Information Security Management System (ISMS) that complies with industry-recognized standards, such as ISO 27001/CEA Guidelines or NIST Cybersecurity Framework or guidelines/standards issued time to time by the competent authority.

b. The Contractor shall implement and ensure all requirements, clauses of Information Security Practices mentioned in the POWERGRD’s information security policy, procedure, and manual.

c. The Contractor shall regularly assess and mitigate risks to the security of POWERGRID's data and information, including but not limited to risks arising from cyber threats, human errors, and natural disasters.

d. The Contractor shall implement and maintain appropriate security controls, including but not limited to access controls, network security, malware protection, secure configurations, and security monitoring and logging.

e. All supplied servers, workstations and applicable appliances shall support integration with SIEM, Anti-Virus and SOC monitoring solutions.

f. Logs shall include privileged activities, configuration changes, authentication events, security events and system integrity events and shall support forwarding to central SIEM.

24. Compliance Verification

The Purchaser reserves the right to seek evidence of compliance with the above requirements during the contract period and support lifecycle of the supplied systems. Non-compliance shall constitute a material breach of contract.

Appendix-A

Patch Management

The Contractor shall establish and maintain a secure patch management framework covering operating systems, applications, firmware, BIOS, databases, open-source components, and all cyber security devices supplied under the project. The framework shall support both online and offline patching and enable centralized patch management without requiring individual OT systems to connect directly to the Corporate-IT network.

The Owner shall provide a single controlled connection point to the Corporate-IT network at the Control Centre for downloading patches, firmware updates, antivirus/EDR signatures, and other security updates. No individual OT system shall be directly connected to the Corporate-IT network. Downloaded updates shall be transferred to the OT environment through designated patch management infrastructure and secure communication channels in accordance with the approved cyber security architecture.

Patch repositories and deployment servers shall be segregated in accordance with the approved cyber security architecture. All patches, signature updates, and firmware upgrades shall be obtained only from trusted OEM sources, verified for integrity, tested on a designated test environment, and deployed only after successful validation and approval.

The latest available patches shall be applied prior to Factory Acceptance Testing (FAT). Throughout the Maintenance period, the Contractor shall provide and manage security patches, firmware updates, antivirus/EDR definitions, and security signatures for all supplied systems and cyber security devices. Updates for cyber security systems shall be carried out through approved offline mechanisms.

The Contractor shall assess, mitigate, and remediate identified vulnerabilities throughout the project lifecycle. For vulnerabilities where patches are unavailable, OEM-recommended compensating controls and mitigation measures shall be implemented. A documented rollback mechanism and backup of at least the last two system configurations shall be maintained.

Patch deployment timelines shall be in accordance with the CEA (Cyber Security in Power Sector) Regulations, 2026, and applicable guidelines. Critical and zero-day vulnerabilities shall be addressed on priority following validation on the test environment, while vulnerability notifications and corrective actions shall be communicated to the Employer without delay.

Any modifications required to maintain system performance, reliability, or functionality following patch deployment or firmware upgrades shall be carried out by the Contractor at no additional cost to the Employer.

Appendix-B

Cyber Security and System Hardening Policy:

- No application software other than meant for/ required for OT system shall be installed without prior approval of employer/owner.
- Process controls systems shall be designed, configured, operated, and maintained to provide only required functions. Operating System services and components not required for safe and secure operation of Control System should be disabled / uninstalled. All unused default operating system users shall be disabled.
- All the Hardware, Operating Systems (OS) and application software shall be hardened based on industry standards and best practices. List of ports and services enabled in each hardware device must be shared after SAT. This list must be updated periodically if any new ports/services are allowed or blocked after prior approval of Owner.
- Whitelisting policy shall be deployed for all software, services, port configuration, network routing, data flow, access etc. and all these details shall be documented, and any changes shall be recorded and informed to owner during entire period of contract. List of ports and services enabled in each hardware and software must be updated periodically during Maintenance Period if any new ports/services are allowed or blocked after prior approval of Owner.
- Systems under operation shall not be run in administrator mode in normal operations. Administrator mode should only be used for specific administrative requirements.
- Usage of USB devices and Wi-Fi dongles is strictly prohibited. USB / Bluetooth Tethering shall be disabled in all servers and consoles.
- Transferring information from OT network is to be done only as per approved procedure for secure transfer of data.
- Anti-virus shall be installed in computers and laptops used in OT network. Laptops which are not registered and labelled shall not be connected to OT network.
- Any software/application/OS which is to be downloaded from OEM's website, its integrity check using hash SHA256 calculation should be done and verified by the contractor before installation.
- RDP, SMB and other remote administration services shall be disabled where not required and otherwise restricted through approved security controls only within network.
- All default user id & passwords shall be changed. All default user id & passwords shall be changed periodically in coordination with employer as per their policy. Default user settings shall enforce password complexity and usage rules.
- Secure digital certificates shall be supported and configured
- Password Managers shall be used to store passwords in encrypted format and use it to perform any logins into the system.
- Any user created for system, or application shall not contain the word "admin" in it.
- Uniform IP address documents shall be maintained.
- Login banners with configurable warning text shall be provided for all operating systems.
- The Contractor shall configure each component of the procured product to operate using the principle of least privilege. This includes operating system permissions, file access, user accounts, application-to-application communications, and system services.
- Implement trusted, un-trusted and DMZ with clear perimeters.

- Spanning tree protocol shall be used in LAN devices to ensure stability in network when a device is removed or added.
- User authentication shall be done considering the best practices in cyber security.
- All Unused ports (physical and logical) of all devices such as on switches, routers, firewalls, consoles, servers etc. shall be disabled.
- All unused services shall be disabled by default. There shall be a provision to turn on all services on request.
- All the devices that connected to the system through LAN shall have mac-based binding. In routers & switches, only the specified/required IP addresses should be OPEN.
- Host-based firewalls shall be configured to only allow connections from specified nodes.
- All the communication should be done through secure protocols such as SFTP, HTTPS etc. All communication with system constituents shall be encrypted on application level, as applicable.
- For web-based systems, compliance with OWASP Top 10, API security assessment, and secure session management shall be ensured.
- Implement proper Access matrix (Access Control List-ACL) to prevent unauthorized access to resources / pages / forms in website.
- Do not reference components (such as javascripts, stylesheets etc.) directly from third-party sites.
- Store critical data such as secret keys, passwords, certificates etc. in encrypted form in the database.
- Prevent critical information from public access
- Hash the password before it is relayed over network, or is stored in database.
- Implement proper Session Timeout
- Assure admin/Super-Admin URL's is/are accessible from restricted IP's only.
- Assure third-Party links/page (partial/full) open in different tab, with a disclaimer.
- Disable directory listing.
- Implement Logout buttons in all authenticated pages
- Use the latest and non-vulnerable versions of Application Server (IIS/Apache etc.)
- Firewalls shall be configured with:
    - Clean-up rule: Place a 'Deny Any-Any' rule at the end of the rule base. o Never create an 'Allow any-any' rule.
    - Allow rules should be created only for required services.
    - This will result in all traffic being disallowed, unless specifically allowed.
    - Lockdown/stealth rule o All traffic destined for the firewall itself should be disallowed. Administrative access to security appliances shall be restricted to authorized management networks.
    - Anti-spoofing rule. o Place anti-spoofing rule as per RFC 1918 and 2827.
    - Enable DoS/DDoS features on Firewall o Enable application-level filtering of firewall o It should show policy traffic trend over the day with host and destination o addresses by selecting on each policy.
    - Geofencing shall be enabled in all the firewalls and security devices.

- Routers shall be configured with: o Deploy proper access management and avoid remote administration. o Enable secret password.
- Change default SNMP community string.
- ACLs (Access Control Lists) shall include o Apply egress/ingress filter o Filter all RFC 1918, 3330 address space and special/reserved address o Permit the required services for the required IP addresses only o Deny everything else.
- Area segregation must be implemented (if OSPF is being used) between internal and external networks. Appropriate protocols must be enabled to prevent networks loops

Note: The applicability of the above requirements shall be based on project-specific operational needs and the Employer's policies. Compliance with the Employer's Cyber Security Policy and System Hardening Policy shall be included and ensured by contractor. The same shall be finalised during detail engineering.

Appendix-C

Software Inventory

An inventory of all software including open-source components as per CERT-In guidelines and its license details shall be maintained by the Contractor. The Contractor shall submit the following inventory lists:

a. Preliminary inventory list at the time of the FDS approval,
b. An updated inventory list immediately prior to the start of the FAT,
c. And the final inventory list at the time of system commissioning.
d. Checksum/Hash for all supplied Software for Software Integrity Check.
e. Version Management

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

The Contractor shall also submit the inventory list in line with Technical Guidelines on SOFTWARE BILL OF MATERIALS (SBOM) as per CERT-In guideline (**CERT-In Technical Guidelines on SBOM, QBOM & CBOM, AIBOM and HBOM Version 2.0)** for approval and shall include the following minimum details:

S.No.	Data Field	Description
1	Component Name	The name of the software component or library included in the SBOM.
2	Component Version	The version number or identifier of the software component.
3	Component Description	A brief description or summary of the functionality and purpose.
4	Component Supplier	The entity or organization that supplied the software component.
5	Component License	The license under which the component is distributed, including terms.
6	Component Origin	The source or origin: proprietary, open-source, or thirdparty vendor.
7	Component Dependencies	Other components or libraries it depends on, including names and versions.
8	Vulnerabilities	Known security vulnerabilities, severity ratings, CVE references.
9	Patch Status	Indicates if patches or updates are available for known issues.
10	Release Date	The date when the component was released or made available.
11	End-of-Life (EOL) Date	The date when support or maintenance is scheduled to end.
12	Criticality	Importance to overall functionality or security: critical, high, medium, low.
13	Usage	Export control restrictions or intellectual property rights.

	Restrictions	
14	Checksums or Hashes	Cryptographic checksums or hashes to ensure integrity and authenticity.
15	Comments or Notes	Additional comments, notes, or annotations.
16	Author of SBOM Data	The entity that creates the SBOM data for this component.
17	Timestamp	Record of the date and time of the SBOM data assembly.

Note:

1. It is preferred that the above data fields be structured, maintained, and shared in SPDX format for compatibility and interoperability.
2. The above table is indicative only. The format and data fields shall be finalized during detailed engineering stage.

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

   The SBOM and inventory shall be maintained by the contractor during entire contract period.

   The Opensource components should be maintained with following Information:

Open-Source component	**License**	**Baseline version**	**Git repository link**	**Deployed version**	**Latest version available**	**Checksum**

Hardware Inventory

The contractor shall submit hardware inventory of all hardware supplied under this project as per CERT-In guidelines.

The Contractor shall also submit the inventory list in line with Technical Guidelines on Hardware BILL OF MATERIALS (HBOM) as per CERT-In guideline (**CERT-In Technical Guidelines on SBOM, QBOM & CBOM, AIBOM and HBOM Version 2.0)** for approval and shall include the following minimum details:

S.No.	Data Field	Description
1	Product Name	The common or marketing name of the hardware item.
2	Product Version	The specific iteration or release number of the product.
3	Product Details	Key specifications and features that describe the hardware.
4	Warranty/AMC	Information regarding the product's guarantee and any annual maintenance contract.
5	Manufacturer Name	The name of the company responsible for producing the hardware.
6	Manufacturer Location	The geographical address of the product's manufacturer.
7	Manufacturing Date	The specific date when the product was produced.
8	Supplier Information	Details about the company that provided or sold the product
9	Supplier Location	The geographical address of the product's supplier.
10	Model Number	A specific alphanumeric identifier for a particular product design.
11	Serial Number	A unique identifier assigned to each individual unit of a product for tracking.
12	Technical Specification	Detailed technical characteristics and performance parameters of the component (e.g., voltage, frequency, capacity).
13	Supplier Information	The name and contact details of the company that supplied the component to the manufacturer of the larger product.
14	Supplier Location	The geographic location (city, country) of the direct supplier of the component.
15	Technology Node	For integrated circuits, this refers to the semiconductor manufacturing process technology (e.g., 7nm, 14nm), indicating its feature size and generation.
16	Compliance	Declarations or certifications indicating adherence to relevant industry standards, regulations, or environmental directives (e.g., RoHS, CE).
17	Power supply	Details about the component's power requirements, such as voltage, current, and wattage.

18	License Information	Any associated intellectual property licenses or usage terms, particularly relevant for firmware or embedded software within the component.
19	Subcomponent	This refers to the recursive nature of an HBOM; if a component itself contains further distinct hardware parts, those would also be listed with similar detailed attributes.

The above table is indicative only. The format and data fields shall be finalized during detailed engineering stage**.**

Appendix-D

Declarations & Formats

Index

- Declaration format for SBOM and HBOM
- Malicious Code declaration format during detail engineering
- NDA Format during commissioning/AMC
- Malicious Code declaration format before FAT
- End of Life declaration format from respective OEM
- End of Life declaration format from contractor
- MUTUAL CONFIDENTIALITY AGREEMENT

Declaration format for SBOM and HBOM

Name of OEM: Date:

Project Name:

NOA Reference:

Subject: Declaration for Submission of SBOM and HBOM as per CERT-In guidelines

We, **[OEM Name]**, hereby declare that all products, software, and hardware supplied to **[Organization Name]** comply with the requirements outlined in the **CERT-In Technical Guidelines on SBOM, QBOM & CBOM, AIBOM and HBOM Version 2.0**, issued by the Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Government of India.

We also confirm that , we will submit the SBOM and HBOM as per mentioned in CERT-In guidelines (TechnicalGuidelines-on-SBOM,QBOM&CBOM,AIBOM_and_HBOM_ver2.0.pdf) during detail engineering prior to design approval.

(Authorised Signatory)

Name/ Designation/ Address of the firm

Seal of the firm

Date:

Place:

Malicious Code declaration format during detail engineering

Name of OEM: Date:

Project Name:

NOA Reference:

Subject:

1. This is to Certify that the Hardware and Software being offered as part of the contract does not contain embedded malicious code that would activate procedures to:

(a) Inhibit the desired and designed function of the equipment.

(b) Cause damage or corruption [includes physical / software / data] of or to the user
or equipment by way of malicious exploit.

(c) Tap information resident or transient in the equipment / networks.

2. The contractor will be considered to be in breach of the contract, in case physical damage, corruption or loss of software / data or infringements related to copyright and Intellectual Property Rights (IPRs) are caused due to activation of any such malicious code in embedded software.

(Authorised Signatory)

Name/ Designation/ Address of the firm

Seal of the firm

Date:

Place:

NDA Format during commissioning/AMC

---- TO BE FILLED BY Contractor REPRESENTATIVE AT SITE DURING COMMISSIONING / MAINTENANCE----

DECLARATION OF CONFIDENTIALITY

I acknowledge that, in my capacity as a member (or staff, employee) of ..... I will have access to certain Confidential Information (as defined in Agreement between Owner and M/S .....) of Owner, which may be in oral, written or any other form.

I understand that all _____ members must sign a Declaration of Nondisclosure when they commence their association with the _____. Under this declaration, members consent to keep all matters to which they are privy related to all projects being conducted at the _____ confidential.

I agree that during my association with the Project relating to Owner and after the competition/termination of Project, I shall not disclose to any other person, firm or corporation, any confidential information relating to Owner's Company.

I also understand that I am required to notify _____ of the _____ or his/her designate immediately of any breach of my obligations or conflict of interest under this agreement which comes to my attention.

By signing and returning a copy of this document, I confirm my understanding and acceptance of the above clause and will comply with these clauses. I also agree that my obligation to comply with the above will survive my termination of association with the M/S in future.

_____

Contractor Representative Signed: _____

Contractor Representative Name (printed): _____

Sign and Name of Owner's Executive as Witness: _____

Seal of the firm

Date:
Place:

Malicious Code declaration format before FAT

Name of OEM: **Date:**

Project Name:

NOA Reference:

We hereby confirm that the any imported equipment/material/item/parts/component (comprising of embedded systems) to be supplied under the contract shall be tested in the certified laboratories to check for any kind of embedded malware/trojans/cyber threats and for adherence to Indian Standards as per the directions issued by Ministry of Power/Govt. of India from time to time.

In case of such import from specified "prior reference" countries, the requirement of prior permission from the Govt. of India including protocol for testing in certified and designated laboratories by Ministry of Power/Govt. of India shall also be complied.

We hereby confirm that the above test details & compliance shall be submitted prior to Factory Acceptance Test (FAT).

We also confirm that the list out the products and components producing Toxic e-waste under the contract and shall furnish to the Employer the procedure of safe disposal at the time of closing of the contract.

(Authorised Signatory)

Name/ Designation/ Address of the firm

Seal of the firm

Date:

Place:

End of Life declaration format from respective OEM

Name of OEM :……. **Date:**

Project Name:

NOA Reference:

We hereby confirm that we shall ensure that the **(Name of Equipment)** supplied to M/s contractor under "Project Name*"* is having support (including updates & patches) for a period of _____ years (as specified on the technical specification) from the **Operational Acceptance (OA)** as specified in technical specifications.

We also confirm that the (**Name of equipment**) is current industry standard model and the equipment has not established a date for termination of its production.

Details of Hardware

1) Complete Model No:

The documentary evidence certified by us for the validity of End-of-Life/ End-of-Support is also attached.

(Authorised Signatory)

Name/ Designation/ Address of the firm

Seal of the firm

Date:

Place:

End of Life declaration format from contractor

Name of OEM:…….

Project Name:

NOA Reference:

We hereby confirm that the (**Type of Product**) supplied under "*Project Name*" **(hardware & applications)** are current industry standard models and the equipment manufacturer has not established a date for termination of its production and are available with more than one supplier locally.

The Obsolescence details of (hardware and applications) for patch/updates (Select one): **Declared/ Not Declared.** (Provide details if "Declared").

We also hereby confirm that we ensure with OEM that the service & support (including updates & patches) for all software and hardware supplied under this project for a period of _____ years (as specified on the technical specification) from **Operational Acceptance (OA)**.

(Authorised Signatory)

Name/ Designation/ Address of the firm

Seal of the firm

Date:

Place:

Appendix-NDA (Non-Disclosure Agreement)

MUTUAL CONFIDENTIALITY AGREEMENT (to be signed on Stamp/e-stamp)

THIS AGREEMENT is made on the ---- day of ---------- between **Power Grid Corporation of India Limited (POWERGRID),** a company incorporated in India and having its Office at B-9, Qutab Institutional Area, Katwaria Sarai, New Delhi-110016 AND ----------. incorporated under the laws of India and having its principal place of business at ----------.

For purposes of this Agreement, the party that owns and/or discloses confidential information is hereinafter referred to as the "Disclosing Party" and the party that receives and or accesses confidential information hereunder is hereinafter referred to as "Recipient."

1. **Purpose.** The parties hereto wish to explore a business opportunity of mutual interest and in that either party may receive confidential information of the other party for the following purposes: ---------- at **POWERGRID.**

2. **Definition.** "Confidential Information" means any information, technical data, or know how (including, but not limited to, information relating to research, products, software, services, development, inventions, processes, engineering, marketing, techniques, customers, pricing, internal procedures, business and marketing plans or strategies, finances, employees and business opportunities) disclosed by the Disclosing Party to Recipient either directly or indirectly in any form whatsoever including, but not limited to, in writing, in machine readable or other tangible form, orally or visually (subsequently reduced to writing) (i) that has been marked as confidential; (ii) whose confidential nature has been made known by Disclosing Party, orally or in writing, to Recipient; or (iii) that due to its character and nature, a reasonable person under like circumstances would treat as confidential.

3. **Exclusions.** Confidential Information does not include information, which: (i) is in Recipient's possession at the time of disclosure; (ii) before or after it has been disclosed to Recipient, becomes part of the public knowledge or literature, not as a result of any action or inaction of Recipient; (iii) is approved for release by written authorization of the Disclosing Party; (iv) is disclosed to Recipient by a third party not in violation of any

obligation of confidentiality; or (v) is independently developed by Recipient without reference to Confidential Information of the Disclosing Party.

4. **Use Limitations**. Recipient agrees not to use the Confidential Information for its own use or for any purposes except for the Purpose expressly set forth above. Recipient agrees not to copy, alter, modify, disassemble, reverse engineer or decompile any of the materials unless permitted in writing by the Disclosing Party.

5. **Non-Disclosure.** Recipient agrees not to disclose the Confidential Information to any third parties or to any of its employees except those employees who have a need to know the Confidential Information for accomplishing the stated Purpose described herein and where such employees shall be made aware that the information is confidential and shall be under a written contractual restriction on non-disclosure and proper treatment of Confidential Information that is no less restrictive than the terms of this Agreement. Notwithstanding the foregoing, Recipient may disclose the Disclosing Party's Confidential Information to the extent required by a valid order by a court or other governmental body or by pursuant to an applicable law or regulation; provided, however, that Recipient will use all reasonable efforts to notify Disclosing Party of the obligation to make such disclosure in advance of the disclosure so that Disclosing Party will have a reasonable opportunity to object to such disclosure. Recipient agrees that it shall treat the Confidential Information with the same degree of care as it accords to its own confidential information of a similar nature; provided that in no event shall Recipient exercise less than reasonable care to protect the Confidential Information. Recipient agrees to advise the Disclosing Party in writing of any misappropriation or misuse by any person of such Confidential Information of which Recipient may become aware.

6. **Third Party Information.** Neither party shall communicate any information to the other in violation of the proprietary rights of any third party.

7. **Return of Materials.** Any materials or documents of Disclosing Party which are furnished to Recipient, and all copies thereof, at the earlier of Disclosing Party's request for return of the materials, or the termination of the business relationship between the Disclosing Party and Recipient, at the Disclosing Party's option, will either be: (i) promptly returned to the Disclosing Party; or (ii) destroyed by Recipient (with Recipient providing written certification of such destruction).

8. **No License.** The Confidential Information shall remain the sole property of the Disclosing Party. No license is granted to Recipient under any patents, copyrights, mask work rights or other proprietary rights by the disclosure of any information hereunder, nor is any warranty made as to such information.

9. **Remedies.** Recipient understands and agrees that the Disclosing Party is providing the Confidential Information to Recipient in reliance upon this Agreement, and Recipient will be fully responsible to the Disclosing Party for any damages or harm caused to the Disclosing Party by a breach of this Agreement by Recipient or any of its officers, directors, employees or consultants. Recipient acknowledges and agrees that a breach

of any of its promises or agreements contained herein will result in irreparable injury to the Disclosing Party for which there will be no adequate remedy at law, and the Disclosing Party shall be entitled to apply for equitable relief, including injunction and specific performance, in the event of any breach or threatened breach or intended breach of this Agreement by Recipient. Such remedies, however, shall not be deemed to be the exclusive remedies for any breach of the Agreement but shall be in addition to all other remedies available at law or in equity.

10. **Attorneys' Fees, Jurisdiction/Venue.** In the event of any litigation or other legal proceedings between the parties, the prevailing party shall be entitled to reasonable attorneys' fees and all costs of proceedings incurred in enforcing this Agreement. The Courts in Delhi, India shall have exclusive jurisdiction to try and dispose of any proceedings arising out of this Agreement.

11. **Termination & Survival.** This Agreement will become effective as of the date first mentioned herein above and will continue to be in force for a period of one (1) year thereafter. Recipient’s obligations under this Agreement with respect to Confidential Information it has received shall continue for a period of Nine (9) years after such disclosure.

12. **General.** This Agreement sets forth the entire understanding and agreement of the parties with respect to the subject matter hereof and supersedes all other oral or written representations and understandings. This Agreement may be amended or modified only in writing signed by authorized representatives of the parties hereto. If any provision of this Agreement is found by a proper authority to be unenforceable or invalid, such

unenforceability or invalidity shall not affect the other provisions of this Agreement and the unenforceable or invalid provision shall be construed to be amended in order to avoid such unenforceability or invalidity while preserving as closely as possible the intent of the parties.

13. **Notices.** All notices or reports permitted or required under this Agreement shall be in writing and shall be by personal delivery, nationally recognized overnight courier service, facsimile transmission or by certified or registered mail, return receipt requested, and shall be deemed given upon the earlier of actual receipt or one (1) day after deposit with the courier service, receipt by sender of confirmation of electronic transmission or five

(5) days after deposit in the mail.

IN WITNESS WHEREOF, each of the parties hereto have caused this Agreement to be executed by a duly authorized representative of such party as of the date first above written.

Power Grid Corporation of India Limited

……

Signature: _____

Name: ……

Title: ……...

Date: …….

Signature: _____

Name: ……

Title: ……

Date: ……...