Design, Manufacturing, Supply & Installation, Testing & commissioning of Supervisory Control &Data Acquisition System for IMT Manesar industrial area at Sub-Station level associated with 220KV/66KV/11KVSubstation Sector 1, 2, 3, 4, 8 & Old Manesar and distribution level on all 11KV General Industrial and Independent Industrial/NDS feeders under the jurisdiction of 'OP' Circle-I,

DHBVN, Gurugram, (Haryana)-(BID NO. TSGP-07/2017-18)

Ref: Pre Bid Meeting Held on 9-10=2017 at DHBVN office, Hetri House, Gurgoan

Clarification on the SCADA functionality (part of pre-bid discussions)

The operational requirements of SCADA have been elaborated in chapter 5 of Vol-II and clarification to the various points raised by the bidders, have been provided separately. The operational requirements have been explained during the pre-bid discussions.

The following clarifications are provided and should be considered by bidders for this project.

1. System Software Requirements :

All SCADA applications as defined in the tender document shall use manufacturer supplied software utilities and documentation. The software design shall be proven which will fulfil all desired functions and software coding standards shall address the following:

(a) Software's shall be designed to accommodate the ultimate size of SCADA system as proposed and shall meet all desired functions. It shall have the capability for expansion as required.

(b) Software shall be modular so that the changes to the program application can be done in a modular fashion without altering the basics, it should be easy & less time consuming to change the program in required modules.

(c) Functions taking long execution times shall recognize and process user requests to abort the processing under user termination command.

(d) Programming languages: The software shall be written using ISO or ANSI or ECMA standard programming languages like C, C++, VB, JAVA and SQL and for UNIX based systems the APIs shall be POSIX-conforming. This shall be confirmed by the bidder in this technical bid.

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

(f) Architecture shall enable interaction of applications from different product manufacturer, platforms etc.

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

2. System Software Requirements :

The SCADA system shall maintain Time and date for use by various software applications. The GPS based time receiver shall be used for synchronizing the SCADA system time and all clocks shall be synchronized with an accuracy of 100 mms (+ /-). The SCADA shall include two redundant time and frequency standards. Failure of the online unit shall result in automatic switching to the redundant unit. The SCADA shall periodically check if the backup unit is operational and failure of either unit shall be alarmed. The time and frequency standard unit shall support a common time code output format. The equipment shall have protection from lightning like surge protection system

3. NetworkServices

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

(a) Network file management and transfer, for files containing text, data, and/or graphics information

(b) Network printing management

(c) Network time synchronization

(d) Network backup over LAN

(e) Task-to-task communications to external computers

(f) LAN global naming facilities.

(g) Remote procedure call

(h) Remote terminal session

4. SecurityServices

Firewalls i.e. LAN Firewall & Gateway Firewall, intrusion Prevention system IPS The SCADA system shall have a comprehensive security solution for secured zone

(Network based & Host based) Authentication (multi layered), LDAP, and Encryption mechanism. The bidder shall incorporate a suitable integrated intrusion detection system to detect the intrusions and prevent the system from such intrusions.

Followings are the functional requirement from the security system:

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

ii. Firewalls shall be Robust, Secure, Scalable and future-proof with Centralized Management.

iii. LAN Firewall shall provide isolation/security services between the subsystems installed under SCADA – SAS system

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

v. LAN Firewall shall provide isolation/security services between the subsystems installed under SCADA – SAS system.

vi. Two types of IPS Host based & Network based shall be deployed with minimum hardware & they should not go blind in peak traffics. vii. IPS should have hybrid technology to detect attacks. It should detect through a combination of Protocol Anomaly and Signature matching.

viii. Shall have Gateway antivirus which will protect from inflow of virus from the Internet and other WAN locations at the gateway itself with content filtering without any lag in data transmission. ix. Shall have strong authentication containing user name and passwords which shall be very difficult to compromise.

x. SSL over VPN to provide secured link over public network such as with RTU.

4.1 Followings are the features specific to each component of security system

Firewall:

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

i. Firewall speed >250 Mbps

ii. Data encryption supported DES (56 bits) 3 DES (168 bits) and hashing algorithm like MD5 and SHA-1

iii. It shall have minimum 8 Ethernet 10/100 /1000 ports (4ports for connectivity to two web servers & 4 Ports for connectivity to LAN

iv. It shall have capability of working in Load sharing and hot standby mode

v. Encryption to offload the main CPU

vi. Support NAT and PAT

vii. DNS guard features

viii. JAVA and ActiveX blocking

ix. Web based management interface

x. Inspection for web, mail, SQL application etc.

xi. Shall have system logging and accounting feature

xii. No. of concurrent TCP Sessions supported shall be more than 5000, this shall be defined by the bidder.

Intrusion Prevention System (IPS):

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

Both Network based and Host based IPS should have centralized Management Console system which will be either the application server with NMS. The Centralized management console shall have integrated event database & reporting system & it must be able to create and deploy new policies, collect and archive audit log for post event analysis. The system shall have Integrated Event Database & Reporting System.

Automated Update of the signature during the entire contract period shall be provided and there should be provision for creating customized signature

Intrusion Prevention System (Network Based)

After detecting any intrusion attempt there should be provision to configure to perform the following functions:

i. Capability for Detecting the intrusion attempt that may take place, intrusion in progress and the intrusion that has taken place
ii. Reconfigure the firewall

iii. Beep or play a .WAV file
iv. Send an SNMP Trap datagram to the management console. The NMS server envisaged under the specification shall be used as management console also.
v. Send an event to the event log.
vi. Send E-mail to an administrator to notify of the attack.
vii. Save the attack information (Timestamp, intruder IP address, victim IP address/port, protocol information).
viii. Save a trace file of the raw packets for later analysis ix. Launch a separate program to handle the event
x. Forge a TCP FIN packet to force a connection to terminate. xi. Detect multiple forms of illicit network activity: -Attempted
xii. Vulnerability Exploits -Worms -Trojans -Network Scans -Malformed Traffic Login Activity

The System shall support monitoring of multiple networks. The system shall also support the monitoring of additions or changes to addresses of devices on the network.

Intrusion Prevention System (Host Based)

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

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

Should provide events check for suspicious file transfers, denied login attempts, physical messages (like an Ethernet interface set to promiscuous mode) and system reboots.

5. Software Maintenance and Development Tools

General requirements

A set of software shall be provided to enable maintenance of application software and development of new software in software development mode. All hardware and software facilities shall be provided to allow creation, modification and debugging of programs in all languages that are supplied. The following shall thus be possible:

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

The following features shall be provided:

- Library management
- Programs allowing to copy and print any data or program files
- Backup and restore
- File comparison
- Sort and merge
- Programs that allow to partially save and recover volumes
- Core and memory dump

Code Management

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

The code management feature shall include inventory, version, and change control and reporting features. The code management facility shall retain a complete history of additions, deletions, and modifications of library files.

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

6. Database Development software

The databases organization shall be designed to meet the following major functional requirements of Data consistency, Compliance with the system performance requirements including both response times and expansion capabilities,

A Database development software shall be provided which shall contain database structure definitions and all initialization data to support the generation of all relational, real time database (RTDB) non-relational run-time databases required to implement the functions of SCADA system. All the facilities required for generating, integrating and testing of the database shall be provided with the SCADA system. The delivered SCADA database shall be sized for the ultimate system as mentioned in the tender document required to fulfil all functional & operational requirements of SAS & SCADA. The database development facility shall be available on development system comprising of server & workstation.

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

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

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

i. Add, modify, and delete telemetered, non-telemetered, or calculated database items and data sources such as RTUs/FRTUs

ii. Add, modify, and delete application program data & create a new database attribute or new database type

iii. Resize the entire database or a subset of the database and redefine the structure of any portion of the database.

7. Display Generation and Management

Interactive display generation software shall be supplied as part of the SCADA which shall generate and edit the required displays. The display generator shall be available on development system & once the display/ displays creation/ modification activity is complete, the compiled runtime executables shall be downloaded on all workstations/ servers. The display editor shall have the provision for the options generally required like :

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

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

Displays shall be generated in an interactive mode.

8. **Report Generation Software**

The SCADA system shall include report generation software to generate new report formats for SCADA and edit existing report formats. The user shall be guided in defining the basic parameters of the report, such as the report database linkages as symbolic point names, the report format, the report activation criteria, the report destination

(workstation, printer, or text file), and the retention period for the report data. The user shall be able to construct periodic reports and ad-hoc queries via interactive procedures. The capability to format reports for workstations and printers shall be provided. The user shall be able to specify the presentation format for periodic reports and ad-hoc query reports as alphanumeric display format, graphical display format, or alphanumeric printer format. All arithmetic, graphical & logical functions should be possible with the report generation application/ utility. The software shall be complete in all respects to generate a proper sized report both in font, size & shape. All reports shall be editable, printable and repeatable in all respects. The reports shall be saved as proper retrievable files & stored in the specific memory with our altering the originals.

All reports shall be easily accessible, format able in normal work.

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

9. **Software Utilities**

As per the tender document volume I and volume II, bidders shall assess the requirement of software's with great degree of care and understanding so as to ensure that all the SAS-SCADA functions are satisfactorily achieved and implemented. All software utilities required & to be used to maintain SCADA software, whether or not specifically mentioned in the tender document & this document Specification, shall be delivered with the system.

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

Proper utility software shall be supplied to achieve the requirement of control & monitoring functions at MCC and monitoring facility at all 66/11 KV substations. MCC will have two separate work stations, one for SAS covering the applications upto the upstream 11KV breakers and other for covering the application down stream of 11KV feeder breakers.

Auxiliary Memory Backup Utility

A utility to backup auxiliary memory of server and workstation files onto a user selected auxiliary memory or archive device shall be supplied. The backup utility shall allow for user selection of the files to be saved based on Server and workstation. All file information & attributes shall be recorded & updated.

Failure Analysis Utility

Failure analysis Utility shall be provided to produce operating system and application program status data for analyzing the cause of a fatal program failure. The failure information shall be presented in a condensed, user-oriented format to help the user find the source of the failure.

Diagnostic Utility

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

System utilization Monitoring Utility

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

Other Utility Services

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

10. Information Storage and Retrieval

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

The data shall be available all time which can be retrieved for display, review, study, analysis, trending and for report generation. All stored data shall be accessible from any time period regardless of changes made to the database after storage of that data. It should be retrievable from all backup storage devices

The addition, deletion, or modification of data to be collected and processed shall not result in loss of any previously stored data during the transition of data collection and processing to the revised database.

Data compression facility should be possible and accuracy of retrieval be 100%. However, the retrieval of compressed historical streams should be of the same performance levels as normal SCADA retrieval. The ISR should be able to interface to external systems for analytics over SOA / ESB for Integration with IT Systems, over the Enterprise Services Bus & SOA Architecture provided as part of IT SRS. The ISR system shall act as the real interface between SCADA and IT System, where-by the real-time operational system is not affected with a transaction processing system like IT, and the IT Integration efforts will not in any way effect the real-time operationally of SCADA System.

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

It shall be possible to have Real-time database snapshots, Hourly Data tables, Hourly data storage, and hourly data calculation, Historical Information (HI) Data Retrieval and System Message Log Storage and Retrieval

Auto execution sequence /Group control

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

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

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

At any time during the execution of a list, the user shall be able to stop further execution via a cancel feature.

Fail-soft capability

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

Remote database downloading, diagnostics & configuration:

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

10.1 Network Management system (NMS)

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

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

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

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

The NMS software shall provide the following network management capabilities:

(a) Configuration management, Fault management & Performance monitoring.

The network management software shall:

a) Maintain performance, resource usage, and error statistics for all of the above interfaces (i.e. servers, workstation consoles, devices, telephone circuit interface equipment, and all SCADA gateways, routers etc.) and present this information via displays, periodic reports, and on-demand reports. The above information shall be collected and stored at user configurable periodicities i.e. up to 60 minutes. The

Network Management System (NMS) shall be capable of storing the above data for a period of one year at periodicity of 5 minutes.

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

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

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

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

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

11. SCADA Hardware Requirement

General Requirement for Hardware

All hardware features described in the Proposal shall be fully supported by the SCADA applications. The hardware shall be CE/FCC or equivalent international standard compliance and shall meet all international standards.

All hardware shall include self-diagnostic features. On restoration of power after interruption they shall resume operation. All servers, workstations and network equipment's (Switches, routers, firewall etc.) shall be compatible for remote monitoring using secure SNMP Ver. 3.0. All hardware shall support both IPv6 and IPv4 simultaneously.

The configuration of the SCADA shall comprise of distributed computing environment with an open systems architecture. The system should be designed in such a manner that it can adapt / accept hardware/software additions without any problems, whether supplied by the OEM of the SCADA system or obtained from different source. Additional hardware/software may be required for capacity expansion or for up gradation, the changes made should not affect the existing SCADA components or its operation. In case of any such conflit, the bidder shall clearly mention such ambiguities during the technical bid proposal.

To be recognized as a true open computer system, all internal communications among the SCADA Servers and all external communications between the SCADA and other computer systems shall be based on widely accepted and published international or industry standards which are appropriate and relevant to the open systems concept or should have a field proven acceptance among utilities. This applies to the operating system, database management system, and display management system, as well as to

APIs providing standardized interfacing between System software and application software.

The final hardware configuration shall be accepted & approved during detailed engineering. At this bidders are requested to refer to the BOQ and carefully understand the SCADA requirements and consider all hardware requirements for satisfactory operation of the SAS-SCADA system, if not included in BOQ. The bidders shall ensure that at the time of final approval of hardware configuration and BOQ, all the hardware is as per the current industry standard models and that the equipment manufacturer has planned the for termination of its production. The bidders shall be responsible to supply any of the hardware required during the operation of this contract and 3 year thereafter, any hardware changes, except version upgrade in same series, proposed after contract period shall be subject to following:

i. The bidder shall clearly these ambiguities in the technical proposal & any such updates shall be proposed for approval.
ii. The new equipment will be better than the equipment supplied earlier, with comparative advantages, features, parameters to be approved by DHBVN.
iii. Updates proposed will have no additional cost implication.
iv. The supplied software shall not be effected by the new equipment or hardware replacement during the warranty period by bidder.

In this tender document all hardware has been broadly indicated as “Server” and “Peripheral device”. The term “server” (also referred as “processor”) is defined as any general-purpose computing facility used for hosting application functions as defined in the specification. The servers typically serve as the source of data, displays and reports. The term “Peripheral Device” is used for all equipment other than servers. Peripheral device includes Workstation consoles, WAN router, LAN, printer, Time & Frequency system, External Cartridge Magnetic tape drive, VPS, Firewalls etc.

The redundant hardware such as Servers, Firewall etc. shall work in hot standby manner. All the servers and networking equipment (Firewalls, LAN switches etc.) shall be mounted in rack panel.

Servers

The Servers shall have provision for expansion of the Processor, auxiliary memory and Main memory (RAM). Servers shall be mounted in a rack and a management console should be provided for centrally accessing all the servers implemented at that particular location. Proposed servers should allow hardware assisted virtualization and processor multithreading.

All servers shall have dual redundant power supplies, capable to operate on single power supply module. And there shall not be any interruptions in the operation of servers when there is a failure between the two AC Power Supply of the server.

Communication Servers

i) FEP / SCADA Server

The redundant FEP/ SCADA server shall be a functional unit that offloads the task of communication & preprocessing between RTUs / FRTUs & SCADA servers. All RTUs/ FRTUs shall be connected to server through IEC 60870-5-104 link. For any existing RTUs/ FRTUs/Relays /Devices that to be integrated, interface must be available to use existing protocols or the protocol as defined in the tender document. Free slots shall be made available inside the FEP server, so as additional communication boards can be plugged-in to meet the network future expansion. Each channel shall be assigned a different protocol and the front-end shall be able to manage several protocols in parallel.

The redundancy of front-end servers / SCADA server shall allow handling of RTUs/ FRTUs connected either through single channel or redundant channels. In both cases, one FEP server shall be able to take control of all RTUs/ FRTU channels. In order to meet network's expansion behind the full capacity of a pair of FE servers, it shall be possible to connect additional FE servers' pairs to the LANs. Each communication line shall be able to support its own communication protocol. The server shall comply VPN based security for connecting with IEC 60870-5-104 node on public networks. Further the nodes and server shall be self-certified by manufacturers as NERC/CIP compliant to comply with future smart grid requirements.

All FEPs shall not have open ports other than needed for protocol traffic / SCADA traffic, and shall have an audit trace of all login attempts / connection attempts. This FEP shall exchange data through secured VPN and encryption of protocol traffic whether it is a is public network or a dedicated one. The equipment should take control command from designated Master IP address only and no other IP.

The Communication Servers shall be able to process time – stamped data and can be directly connected to GPS device for time synchronization. FEP servers shall have a suitable interface for time synchronization from the GPS based time synchronizing system. This interface shall have the time synchronization accuracy of 1millisecond. The FEP server shall further synchronize the time of the RTUs on IEC 60870-5-104 protocols.

FEP server shall have feature to show the online process of raw data from the RTUs/FRTUs as a protocol test analyzer.

ii) Web servers with Firewalls and IPS

Redundant Web servers shall be provided to allow the access of SCADA system data, displays by outside users. One router shall be provided which shall be connected to the external LAN/WAN communicating SCADA system. The external LAN/WAN users shall be able to access SCADA data through the Web server system through this router. Web servers shall also be provided with host based Intrusion prevention & detection system (IPS). The host-based IPS will be installed in both the Web-servers. The Network based IPS shall be supplied for both the SCADA dual LAN and DMZ dual LAN. All necessary hardware & software for Web Servers with firewalls and IPS shall be supplied by the implementation agency.

Firewall

Two firewalls shall be provided, one between Web servers & SCADA dual LAN and another between Web servers & Web server dual LAN. Specification of the firewall is given in the chapter for software requirements. Contractor shall provide equivalent tools such as Apache etc. for Web servers if UNIX or LINUX O/s is used to meet the security requirement as envisaged in the specification. The web server shall be redundant as provided in the BOQ.

Development system server

A non- redundant server to host Developmental applications shall be provided.

12. Router

Router shall be required for data exchange of SCADA Control Centre with RTU's, and respective IT system (IT Data Centre,). The router shall have the following features:

(a) support the OSI and TCP/IP protocols

(b) support X.21/V.35/G.703 interface for interfacing communication links

Routers shall be required for data exchange of SCADA Control Centers with RTUs at various locations. The data exchange between the two centers shall be primarily over secured network using TCP/IP on Fibre optic link. The router shall support the OSI and TCP/IP protocols. The Routers shall be configurable and manageable through local console port, http interface, NMS software and as any other required interface. The Router shall provide built-in monitoring and diagnostics to detect failure of hardware. The Router shall be provided with LED/LCD indication for monitoring the Operational status. The configuration changes on the Router should take effect without rebooting the router or modules.

Memory

a. Flash: Minimum 8MB and upgradable up to 72MB

b. SDRAM: Minimum 64MB and upgradable up to 320MB

Console Port: 01 No. for configurations and diagnostic tests

LAN/WAN Port: The router shall support variety of interfaces as per the requirement at site like V.24, V.35, E1, Channelized E1 etc. along with following minimum number of ports:

- Two fixed 10/100/1000M high speed Ethernet ports
- Two fixed Serial ports with synchronous speed up to 2 Mbps and with interface support for V.35, V.24 ports
- Two fixed ports of G.703 E1 (2 Mbps) interface
- One AUX port

Total no of ports shall be determined by the connectivity requirement and shall be in the scope of bidder.

Scalability: Should have provision of at least 100% additional number of free ports for future scalability

Network Protocol: TCP/IP and support for IP version 6. Shall provide IP address Management

Routing Protocol: RIP v1 (RFC 1058), RIPv2 (RFC 1722 AND 1723), OSPFv2 (RFC1583 & RFC 2328), OSPF on demand (RFC 1793), BGP4 with CIDR implementation as per RFC 1771. The implement should be compliant as per RFC1745 that describes BGP4/IDRP IP OSPF interaction. It shall provide Policy routing to enable changes to normal routing based on characteristics of Network traffic. IS-IS protocol support (RFC 1195).

WAN Protocols: Frame Relay, PPP (RFC1661), Multi-link PPP (RFC1717), HDLC/LAPB, Frame Relay support shall include Multi-protocol encapsulation over Frame relay based on RFC1490, RFC 1293 for Inverse ARP/IP, DE bit support

Network Management: SNMP, SNMPv2 support with MIB-II and SNMP v3 with Security authentication. Implementation control configuration on the Router to ensure SNMP access only to SNMP Manager or the NMS work Station.

- RMON 1 & 2 support using service modules for Events, Alarms, History.
- Should have accounting facility & support multilevel access.

- Shall be Manageable from any Open NMS platform.
- Shall support all required protocols, fttp and http & https enabled Management & should have debugging facility through console.
- AAA Authentication support shall be provided via RADIUS (Remote Authentication Dial-IN User Service) and/or TACACS, PAP/CHAP authentication for P-to-P links, 3DES/IPsec encryption with hardware based encryption services.

13. Archive Storage

Archive storage devices shall be used for backup of the SCADA data and software and archival storage for the Information Storage and Retrieval functions.

Storage shall be provided for general back-up purposes and short-term archiving. The suitable drive shall have sufficient capacity for a complete backup of the SCADA data and software (including all source code) without requiring user action to replace filled recording media. A media changer that accepts industry-standard media handling commands is preferred. External storage device with 4mm DAT, 160/320 GB Cartridge magnetic tape drive shall be supplied for taking Backups and performing restores of the Hard disks of any computer. The external tape drive shall have hot-pluggable port for connection to any computer.

14. Local and Wide Area Networks

The implementation agency will be responsible for implementing the SCADA LAN and the connections to the IT-Enterprise LAN/WAN.

15. SCADA Network

Servers, consoles and devices are connected to each other on a local area network (LAN), which allows sharing of resources without requiring any physical disconnections & reconnections of communication cable. Dual LAN shall be formed for complete SCADA system. LAN shall have the following characteristics:

- Shall conform to the or IEEE 802 series standards.
- Shall preclude LAN failure if a server, device, or their LAN interface fails.
- shall allow reconfiguration of the LAN and the attached devices without disrupting operations
- shall be either controlled LAN such as Token passing or uncontrolled LAN such as CSMA/CD

- shall have minimum of forty-eight (48) ports of 10/100/1000Mbps per LAN switch for SCADA LAN
- CAT 6 or better cables shall be used for LAN

User Interface

The user interface shall include all hardware necessary to facilitate optimum user communication with the SCADA and to efficient operational control and monitoring of the power system.

Consoles

A console consists of the following equipment with adequate provisions as per the requirement.

- One or more LCD monitors.
- One alphanumeric keyboard.
- One audible alarm.
- One cursor control device.
- A workstation.

Monitors

Each monitor shall have the following characteristics; monitors that conform to the latest technology and shall be approved by DHBVN.

The Digital TFT monitor shall have flat panel color screen

S.No	Specification	For 24" monitor
1.	Diagonal Viewable size	80" and 25" as per BOQ
2.	Viewing angle	Sufficiently wide horizontal & vertical viewing angles.
3.	Dot Pitch	0.28mm
4.	Resolution	1920x1080 minimum.
5.	Colour support	16 million
6.	Refresh rate	Minimum 75 Hz
7.	On screen control	Yes

8.	Anti-glare & anti-static	Yes
9.	Tilt, swivel	yes

Workstations

The operator Workstation console shall be used as a Man Machine Interface (MMI) by despatcher for interacting with all SCADA system. Operator Workstation consoles shall also be used as development console to take up developmental/maintenance activities such as generation/up-gradation of database, displays etc. Each workstation shall consist of monitors as per BOQ & single keyboard and a cursor positioning device/mouse.

Workstation consists of a console driving single/ dual monitors as defined in the BOQ.

The user shall be able to switch the keyboard and cursor-positioning device as a unit between both monitors of console.

Printers

Except for the output capabilities unique to any printer type (such as extended character sets, graphic print and coloring features), there shall be no limitations on the use of any printer to perform the functions of any other printer. All the SCADA system printers except Logger shall have dual LAN interface either directly or through internal/external print servers. The characteristics for each type of printer are described below:

Black & White Laser Printer: It is a multipurpose printer used to take prints of displays, reports etc. The laser printer shall have the following features.

- shall be black & white laser printer
- have speed of at least 17 pages per minute
- Minimum resolution of 1200 dots per inch
- Landscape and portrait output orientation
- Memory buffer of at least 48 Mbyte
- Shall be suitable for A4 size normal paper

Colour Laser Printer: It is a multipurpose printer used to take prints of displays, reports etc. The colour laser printer shall have the following features.

- shall be colour laser printer
- have speed of at least 10 pages per minute for A3 & 17 pages for A4 in color
- 600 X 600 dpi

- Landscape and portrait output orientation
- Duplex printing
- Memory buffer of at least 128 Mbyte

Other Peripheral Devices

The Supplier shall supply any other peripheral devices or equipment normally provided for operation, software support, and maintenance of the SCADA.

16. Data access through web server

The Web server at Control Center is to function as source of information on the distribution network. It will be accessed by DHBVN user. Any additional client software, if required, at external clients/users ends, the same shall be made dynamically available from Web server for its downloading by these external clients. There shall not be any restriction to the number of clients downloading this software (i.e. Unlimited number of client downloads shall be provided).

The external users shall be licensed users of the DHBVN. The following features are required:

1. The Web servers shall be sized to support at least 20 concurrent external intranet clients/users for providing access to real-time data.
2. External intranet clients/users shall be connected to the web servers through secure authentication such as VPN access. These users shall be denied direct access to the SCADA protected LAN.
3. Internal SCADA users shall not have any dependency on the availability of the

   Web servers.
4. For the purpose of transfer of data/displays/ from the SCADA system to the Web server system, the SCADA system shall initiate a session with the Web server and any attempt to initiate a session by the Web server shall be terminated by the Firewall in SCADA system LAN. Interface between Web server and SCADA zone shall preclude the possibility of external clients defining new data/Report/Displays. For any sessions initiating from the DMZ LAN into the protected LAN, the servers shall be located in a separate DMZ LAN that will be isolated from common applications connected directly to ISP such as email. The Access to these servers from the external web will be through authorization of Virtual Private Network.

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

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

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

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

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

17. Software License and Upgrades

The bidder shall provide all software licenses for all the software being used in Protection IED offered for engineering, IED setting uploading and FDR down loading etc. The license shall be provided on a site license basis and shall be valid for the System /Equipment life cycle. In the case of anti-virus software, the license shall include regular updates.

The Bidder Shall guarantee that all software are defect free and meet the System specifications, and undertake to fix any defects which may arise during the life of the system at no cost to DHBVN.

In case offered IEDs require any additional software for its integration to RTU then the bidder shall provide the same.

All software versions in components shall be the latest official releases as on the date of supply and shall include all software updates etc. released till that date. A certificate to this effect shall be furnished by the bidder at the time of pre-dispatch inspection for each software package. All new software revisions and/or patch updates that are released before the end of the warranty period which addresses system defects shall be implemented on site and the system re-tested to validate system integrity by the bidder at no cost to the owner (This excludes new revisions which provides additional

functionality). The bidder shall periodically inform the designated officer of the Owner about software updates / new releases that would be taking place after the system is commissioned.

Bidder shall train our engineers to guide the upgrading procedures of project files with respect to latest releases.

18. Cyber Security Management.

General Requirements:

In this Document, basic security requirements are described, which shall be considered by the bidder during the system design phase. The requirements are specified should considered by the bidders.

Risk Assessment:

The vendor:

1. The bidder should conduct assessments of risk from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and operations technology system; and

Updates risk assessments on an organization-defined frequency or whenever significant changes occur to the operational technology system or environment of operation, or other conditions that may impact the security of the operational technology system as agreed with DHVBN

Secure System Architecture:

The system shall be designed and build for secure operations. Examples of secure design principles (depending of the criticality) are:

- Minimal privileges/Need-to-know principle: User and system components only possess the minimal privileges and access rights they need to fulfill a certain function. Applications and network services, for example, should not be run with administrator privileges.
- Defense-in-depth principle: Security threats are not mitigated by a single countermeasure only, but by implementing several complementary security techniques at multiple system levels.
- Availability principle: When there is a redundant system, the failure of a single key component should not interfere with the security relevant system functions.

Contact Person:

The vendor provides a contact person, who will be the single point of contact for Operation Technology (OT) related security topics during the system design phase, the project planning and integration phase and throughout the period of system operations.

User Authentication, authorization and Logon Process:

- Users shall be uniquely identified and authenticated with personal accounts.
- Users shall be able to use the same credentials throughout the system perimeter.
- The user shall only have authorization to perform the functions explicitly defined by his role.
- Before allowing any actions the system shall require each user to be successfully authenticated.
- The system shall force passwords with strength configurable by the security administrator according to standards listed.
- Data used for user identification and authentication shall not be provided from sources external to the site SAS-SCADA.
- Security policy configuration and deployment for IEDs shall be made centrally.
- It is mandatory that all operational IEDs shall continue to perform authentication and authorization in all situations, including during a complete loss of communications with the network (Substation network or external network). All the existing unique user accounts shall be available in this case
- If applicable, the following items shall be implemented after paramount consideration of safe system operation and availability issues:
- User sessions should be locked or logged out after a configurable time of inactivity.
- After a configurable number of failed logon attempts a security event message should be logged and the account should be locked out for an configurable amount of time or until unlocked by a security administrator.

Software and Security Tests:

The implementation agency shall perform a detailed security and stress test on the individual system components developed by the supplier as well as on the entire system. The team undertaking these tests shall be independent from the development team. The test procedure and the test coverage shall be cleared with DHVBN. The results of these tests and the associated documentation (software versions and test configuration) shall be provided to DHVBN.

Secure Network Design:

- Critical network segmentation: If applicable and technically feasible the network infrastructure of the system shall be divided into multiple vertical zones with different functions and protection requirements. Where technically feasible the network zones shall be separated by firewalls, filtering routers or gateways. Network connections to external networks, such as the corporate office network, shall exclusively be routed via specifically hardened application proxies.
- Horizontal network segmentation: If applicable and technically feasible the network infrastructure of the system shall be divided into independent horizontal segments (e.g. according to different locations), the segments shall be separated by firewalls, filtering routers or gateways

19. Feeder interconnection procedures

While designing the feeder conversion from Radial to Ring main, contractor shall make all possible design so that it is possible to feed all the feeder section are of all the feeders with alternate source.

In case of fault in any section of the line, faulty section should get isolated and all healthy sections should be energised.

In case alternate sections are faulty, the faulty sections should be isolated and other healthy sections should be energised.

All line sections should have a alternate supply source that should be monitored and controlled through SCADA system from MCC.