

NLCC UPGRADE AND JUNCTIONS SCADA SYSTEMS PROJECT

SCADA Department



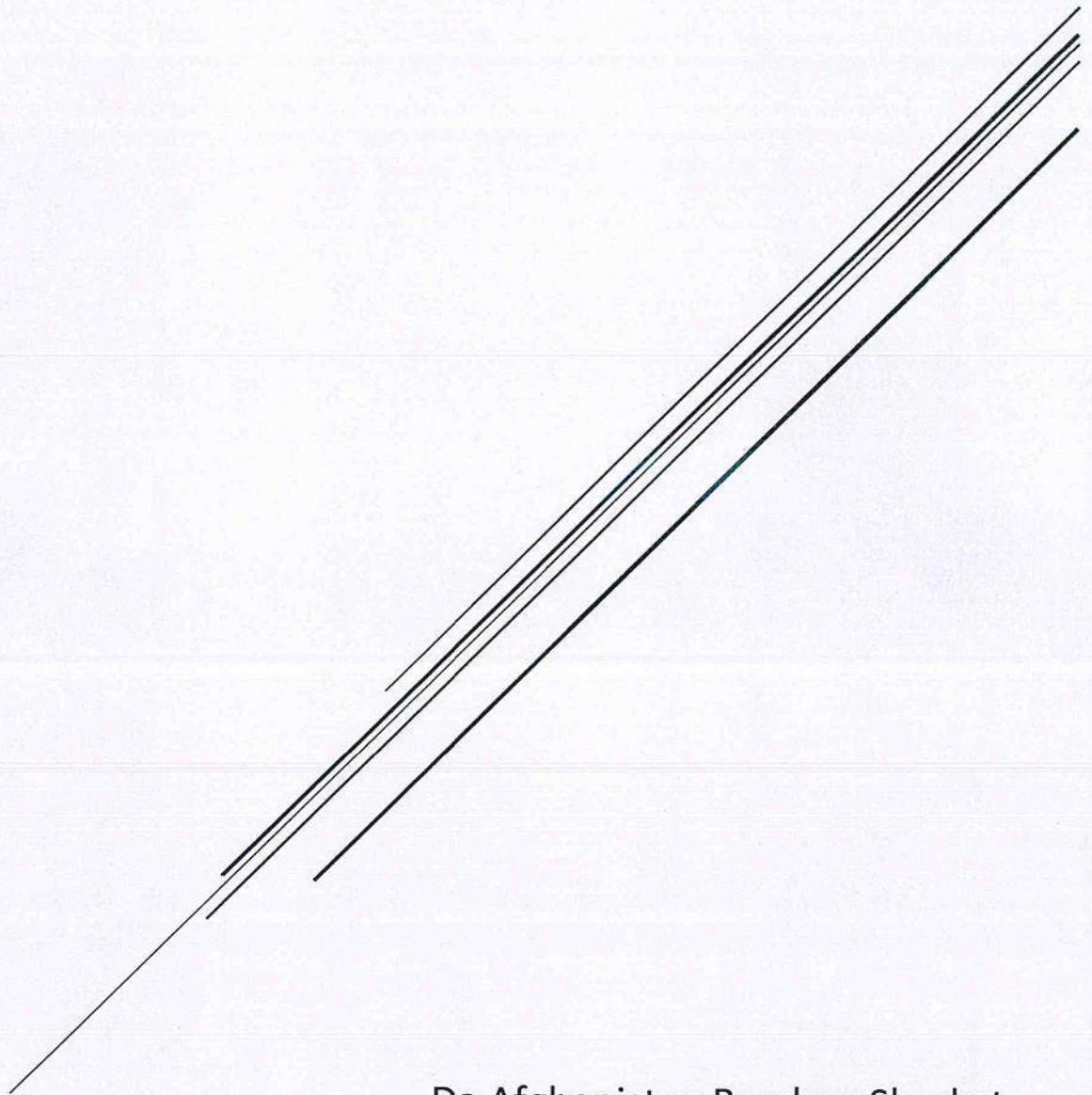
NOVEMBER 6, 2023

DABS

DABS HQ, DIS#3, Kabul, Afghanistan

SECTION 1

NLCC



Da Afghanistan Breshna Sherkat
SCADA Department

SCADA Platform Softwares + Engineering Training

Quantity: 1 Lot

1. System Overview

1.1. System Goals and Objectives

The design of the SCADA system Shall be based on the following goals and objectives:

- a) **High Availability.** The SCADA system architecture shall support dual-, tri-, and quad-redundant configurations that are fault tolerant so that any single hardware failure does not result in the loss of a critical function.
- b) **System Responsiveness.** The high-performance user interface, data collection, and program execution times are provided, as well as the timeliness of making data available to the enterprise.
- c) **Present Pertinent Information.** It is important that the system users have access to a full range of high-quality real-time and historical data, as well as the tools to interpret the data to aid the staff in performing their jobs.
- d) **Expandable/Scalable.** The SCADA hardware and software Shall easily expandable and scalable and provide the capability to upgrade and/or add additional processors, memory, disk units, etc., and expand application programs or add new functions without major disruption to system operation.
- e) **Security.** The SCADA Shall appropriate security features that prevent unauthorized users from accessing the system and permits assigning various levels of access privilege to authorized users. The system also complies with NERC CIP standards and NISTIR 7628 guidelines.
- f) **Advanced Applications.** As operational requirements and needs change, it becomes increasingly important to have good tools to ensure that the electric grid remains secure and is operated as efficiently as possible. The SCADA platform supports several grid security and optimization algorithms, as well as advanced situational awareness features.
- g) **Improved Operator Training.** Operator training simulation tools Shall fully integrated with the products, providing an offline environment for operator training.
- h) **Maintainability.** State-of-the-art auditing, editing, display building, and database generation tools Shall be provided for system maintenance.
- i) **Minimal Customization.** To the greatest extent possible, standard applications Shall proposed to minimize customization to our standard product, thereby lowering the risk of implementation schedule delays and reducing the costs of system procurement and maintenance services.
- j) **Compliance with Standards.** The SCADA platform Shall comply with widely accepted standards for open systems, both from standards organizations as well as de facto standards. This enables utilities to select the best-of-breed hardware and software solutions to meet their future needs and greatly enhances the system's ability to communicate with enterprise systems and take advantage of web-enabling technologies.
- k) **Fully Integrated Platform:** The SCADA platform Shall be a fully integrated modular type to meet the future requirement of DABS for DMS and OMS functionalities. System shall be fully integrated SCADA, OMS, and DMS solution that allows effective operation, monitoring, analysis, restoration, and optimization of critical network operations. The System shall have a single common interface (GUI) for SCADA, OMS and DMS application for all roles for ease of operations, a shared as-operated network model and real-time database for increased performance, and a single hardware platform to simplify IT & OT maintenance and security.

1.2. System Goals Architecture

The SCADA standard system architecture shall be designed to meet the functional, performance, availability, security and expandability requirements of critical systems and to allow the DABS to grow and improve in areas such as customer service and response.

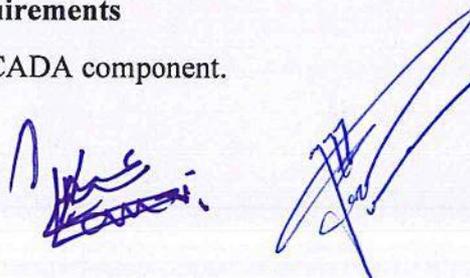
Industry-standard components are used throughout the SCADA system to ensure interoperability with systems from other vendors and to simplify future expansion. The system architecture shall be based on a distributed client/server architecture designed to internationally recognized standards in all areas of interconnectivity. The system architecture shall be based on the OSI seven-layer model, and the network equipment conforms to international standards.

The SCADA System shall support multiple environments as described below:

- a) **SCADA Production System:** The SCADA System shall be in the production environment used for the real-time monitoring and control of the power grid. It performs its function by using real-time data and produces information immediately applicable to real-time operations and represents a "best" estimate of the current "as-operated" real-time state of the power system. SCADA Server with in Built FEP and Communication Server.
- b) **Project Development System:** The Project Development System is an offline environment used for the generation, maintenance and testing of SCADA databases, network model, displays, and reports. Once tested and validated, the updated databases, displays, and reports are published to the production environment for use in real-time operations.
- c) **Training System:** The Training System is an offline environment used for training users in the operation of the system. In this environment, real-time and/or saved data is replaced by equivalent data derived from a "simulation" of the real-time data. A dynamic model of the power system is used to produce the simulation data as the network model responds to hypothetical scenarios consisting of time-dependent loads and contrived system events such as feeder faults.
- d) **Corporate Access System:** The Corporate Access System is a collection of servers that collectively provide web-based access to SCADA functionality to corporate users and external applications connected to the Corporate WAN. They also provide the long-term archive for historical data and reporting. The Corporate Access System is implemented as a demilitarized zone (DMZ); this architecture isolates corporate users and external applications from the SCADA real-time database, thereby minimizing performance issues and data security concerns.
- e) **Quality Assurance System:** The Quality Assurance System is an offline environment used for testing hardware firmware updates, operating system patches, and software upgrades, updates, and hot fixes. The staging environment is a replication of the production environment, and full regression tests are performed in the staging environment prior to updating the production, development, and training environments to ensure all implementation steps and procedures are accurate.

2. SCADA System Functional Requirements

The following section describes the SCADA component.



2.1. Supervisory Control and Data Acquisition (SCADA)

The proposed SCADA system should be able to communicate the communication means available or planned to external devices or systems, the intended protocol (s) to use, the number of points, data concentrators, or RTU description.

2.1.1. Master Station (at the Control Center)

The Proposed SCADA System should be capable of implementing Dual Redundancy Architecture. The master station consists of a host computer (server). Hot-Standby failover redundancy with two host computers (servers). With the Hot-Standby redundancy, the active host computer shall maintain the standby host computers in a fully synchronized state via the TCP/IP network. In the event of a failure of the active host server, the standby server(s) shall automatically assume control of all peripherals, communication lines and services with no action required from the system operator. The Local or Wide area TCP-IP network (LAN or WAN) supporting the host servers' redundancy can be segregated into segments or VLANs to support or coexist with other enterprise services, minimum requirements for the ethernet interface is 1 gigabit/sec data transference capability and 10Mb/sec bandwidth between redundant servers to support the synchronization mechanism of the hosts.

Operator workstations (clients) will be interconnected to the master station server(s) by a Gigabit/sec (minimum requirement) Ethernet local network (LAN) using TCP/IP protocol which will be used for all data exchange services and protocols between the various nodes and devices on the network.

Master Station host server(s) can be implemented in virtual environments following the network and hardware requirements of the servers mentioned in BOQ and sized for the system capacity and specifications according to the number of points, modules, protocols, and requirements of the SCADA hosts servers. The supplier should provide the hardware specifications for a virtualized primary server and for a virtualized secondary server located at a separate facility.

2.1.2. Configuration

The host server(s) and all workstations shall consist of standard PC architecture machines utilizing the latest generation Intel or equivalent processors. The host software and the operator interface software shall run directly in the operating system's own windowing environment. X-Windows sessions, thin clients or other emulations are not acceptable.

For communication with serial-data peripheral equipment, commonly available terminal servers shall be provided to off-load serial communication processing from the host computers.

2.1.3. Communications

The SCADA system will interface with field devices by means of industry standard communication protocols DNP3.0, IEC 870-5-104, IEC 870-5-101, and Modbus. In addition, the system shall have the minimum following protocols available as options:

▪ IEC 61850 (Ed1 and 2)	▪ Allen Bradley Protocol
-------------------------	--------------------------

▪ ASW	▪ L&G 8979
▪ MDO-11	▪ Modbus (RTU and TCP)
▪ QUIN/QUICS IV	▪ RTCS Protocol
▪ SNMP Protocol	▪ Tejas Series V
▪ Goose	▪ Harris 5000/6000
▪ ICCP (Standard, and Secure)	▪ DNP SA (Secure Authentication)

The system shall be able to use a variety of protocols for Data Exchange between systems and interfaces. Protocols such as ICCP, OPC, DNP and IEC60870 family of protocols, and MultiSpeak should be available for Data Exchange tasks.

The above protocols shall be run in native mode, including the secure protocols, there shall be no need for an external protocol converter (hardware unit) or internal converter (third party software driver), nor shall there be any need for any kind of front-end processor.

The master station database editor shall allow the user to define key parameters for each communication line: baud rate, time allowed for an RTU to respond, the number of retries, accumulator poll interval, interval between scans, TLS certificates, and protocol-specific configuration parameters. The communication software shall maintain communication statistics for each RTU. These statistics shall be available as database points so that they can be incorporated in user-defined displays, reports, and alarms.

2.1.4. Security

The SCADA system shall be implemented using industry standard “best practices” and meet all NERC CIP requirements for medium impact control centers in accordance with the CIP version 5 standards. Bidders must detail how they intend to meet each relevant NERC CIP requirement in their proposals.

The following cyber security requirements are based on industry best practices as well as the pertinent requirements for system procurement recommended by the customer’s designated governmental cybersecurity entity (for example, the US Department of Homeland Security). These requirements are intended to provide for a minimum acceptable level of cyber security protection as well as the option for additional levels of requirements which can improve the security posture of the system.

- a) The vendor shall provide cybersecurity features, including but not limited to, authentication, encryption, access control, and communication logging, monitoring, and alarming to protect the system and configuration computer from unauthorized modification or use.
- b) The vendor shall clearly identify the cyber security features and provide the methodology(ies) for maintaining the features, including the methods to change settings from the vendor configured or manufacturer default conditions. The vendor shall not change the standard equipment provided by the third-party OEM in any way that would obligate the user to require service from the vendor.
- c) The vendor shall verify that the addition of security features does not significantly adversely affect connectivity, latency, bandwidth, response time and throughput (including during the SAT when connected to existing equipment).

- d) The vendor shall provide appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.
- e) The vendor shall provide a listing of services required for any computer system running control system applications or required to interface the control system applications. The listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation.
- f) The vendor shall verify and provide documentation that all services are patched to current status. The vendor shall provide, within a pre-negotiated period, appropriate software, and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.
- g) The vendor shall remove and/or disable software components (such as services and executables) that are not required for the operation and maintenance of the control system prior to Factory Acceptance Tests (FAT). The vendor shall provide documentation of what is removed and/or disabled. Examples of the software to be removed and/or disabled may include:
- Games
 - Device drivers for network devices not delivered.
 - Messaging services, Social network file sharing (e.g., MSN, FB, Twitter, IM, etc.)
 - Servers or clients for unused Internet services
 - Software compilers in all user workstations and servers except for development workstations and servers.
 - Software compilers for languages that are not used in the control system.
 - Unused networking and communications protocols.
 - Unused administrative utilities, diagnostics, network management and system management functions.
 - Backups of files, databases and programs used only during system development.
 - All unused data and configuration files.
 - Sample programs and scripts.
 - Unused document processing utilities (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.), unless used and required by the system.
 - Unneeded third-party applications such as Flash Player, Java, PDF viewers, and browser add-ons/plug-ins.
- h) The vendor shall configure hosts with least privilege file and account access and provide documentation of the configuration. The vendor shall configure the necessary system services to execute at the least user privilege level possible for that service and provide documentation of the configuration. The vendor shall document that the changing or disabling of access to such files and functions has been completed.
- i) The vendor shall have a formal patch management and update process for all vendor-supplied software, including operating system and any required third-party applications, and for any vendor-supplied hardware (firmware updates).

MKS
[Signature]

[Signature]
06/Nov/2023

- j) The vendor shall provide details of their patch management and update process. Responsibility for installation and update of patches shall be identified.
- k) The vendor shall provide firewalls and firewall rule sets between network zones or provide firewall rule sets if the firewalls are not provided by the vendor. The vendor shall provide firewall rule sets and/or other equivalent documentation. The basis of the rule set shall be "deny all," with exceptions explicitly identified by the vendor. Note that this information is deemed business sensitive and shall be protected as such.
- l) The vendor shall provide detailed information on all communications (including protocols) required through a firewall, whether inbound or outbound, and identify each network device initiating a communication in accordance with the corresponding rule sets.
- m) The vendor shall recommend which accounts need to be active as well as those which can. The end user shall approve in writing the vendor's recommendation. The vendor shall disable, remove, or modify all the accounts pursuant to the approved recommendation.
- n) After contract award, the vendor shall disable or remove all default and guest accounts prior to FAT. Once changed, new accounts will not be published except that new account information and passwords will be provided by the vendor via protected media.
- o) After the site acceptance testing (SAT), the vendor shall disable, or modify all vendor-owned accounts or negotiate account ownership with the DPDC.
- p) The vendor shall not permit user credentials to be transmitted in clear text. The vendor shall provide the strongest encryption method to commensurate with the technology platform and response time constraints. The vendor shall not allow applications to retain login information between sessions, provide any auto-fill functionality during login or allow anonymous logins. The vendor shall provide user account-based logout and timeout settings.
- q) The vendor shall provide a configurable account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of logins attempts and inactive session logout.
- r) The vendor shall not store passwords electronically or in vendor-supplied hardcopy documentation in clear text unless the media is physically protected. The vendor shall control configuration interface access to the account management system. The vendor shall provide a mechanism for rollback of security authentication policies during emergency system recovery or other abnormal operations where system availability would be negatively impacted by normal security procedures.
- s) The vendor shall provide a system whereby account activity is logged and is auditable both from a management (policy) and operational (account use activity) perspective. The vendor shall time stamp and control access to audit trails and log files. The vendor shall ensure audit logging does not adversely impact system performance requirements.
- t) The vendor shall provide for user accounts with configurable access and permissions associated with the defined user role. The vendor shall adhere to least privileged permission schemes for all user accounts and application-to-application communications.



- u) The vendor shall verify that a user cannot escalate privileges, under any circumstances, without logging into a higher-privileged role first. The vendor shall provide a mechanism for changing user(s) role (e.g., group) associations. After contract award, the vendor shall provide documentation defining access and security permissions, user accounts, applications, and communication paths with associated roles.
- v) Use of browser-based user interfaces for the critical control GUI is not desirable. The primary user interface for the control system should not utilize vulnerable technologies such as native operating system JRE/Java, X-Windows, ActiveX Controls, etc. Vendors shall describe the use of any web-based interfaces for critical control functions. If they are used, vendors should respond to the requirements listed below.
- w) The vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time and throughput (including during the SAT) when connected to existing equipment).
- x) The vendor shall remove or disable all software components and services that are not required for the operation and maintenance of the devices that run an HTTP server prior to the FAT. The vendor shall provide documentation on what is removed and/or disabled.
- y) The vendor shall provide, within a pre-negotiated period, appropriate software, and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

2.1.5. System Sizing

The system software shall be capable of accommodating in its database 1 million Tag Points (at least 250000 external) which includes status and control points, analog input points, text points, communication lines, RTUs, IEDs, reports, graphic symbols.

Vendor shall provide documentation of 99.98% system availability.

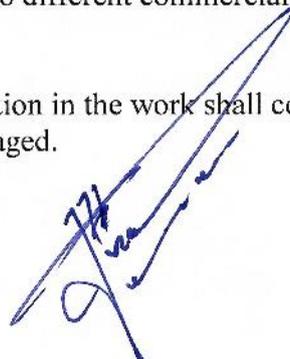
2.1.6. Hardware Platform

The hardware platform encompasses all the physical hardware devices utilized by the SCADA system including host servers, operator workstations (local and remote), storage devices, communication interfaces, printers, GUI devices (LCD Flat Panels) and LANs to which all the hardware devices shall connect.

The system shall be implemented with industry standard general-purpose devices and interfaces. The proposed hardware devices shall be available from at least two different commercial sources (brands) on the market.

All materials and equipment furnished for permanent installation in the work shall conform to applicable standard specifications and shall be new, unused, and undamaged.

2.1.7. Host Servers



The system supplier shall provide the Master Station server hardware and peripherals built by a leading computer industry manufacturer. The preferred computer manufacturer is Dell, the preferred CPU manufacturer is Intel. The servers shall be wholly designed, manufactured, warranted, and assembled by the computer manufacturer. Composite component computer frames assembled with multi-vendor cards by second source manufacturers will not be accepted.

The host servers shall run the latest Microsoft Windows Server 64-bit operating system (OS). Another OS such as UNIX, Linux, OS2, and VMS will not be considered.

The Vendor shall provide OS patch management in accordance with NERC CIP standards. All OS patches shall be evaluated by the Vendor and the results provided to the end user within 30 days of patch release.

The host servers shall utilize Gigabit Ethernet network interface cards (NIC).

The host servers and associated communication equipment shall be delivered rack-mounted in cabinets with perforated walls for easy ventilation.

The Vendor shall provide an option for running the server application on a VMware platform.

The Vendor shall provide at least three (3) customer references where the SCADA server application is running on a VMware platform.

2.1.8. Workstation Consoles

The system supplier shall provide workstation console hardware and peripherals built by a leading computer industry manufacturer. The computer manufacturer shall be the same as for the host servers. The workstations shall run the latest version Microsoft Windows 64-bit operating system. The workstation consoles shall utilize Gigabit Ethernet network interface cards (NIC).

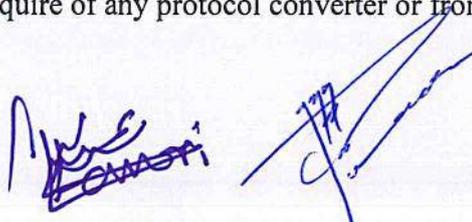
The system shall be able to support any number of workstation consoles without any need for upgrading the system hardware and software.

2.1.9. Data Acquisition

The SCADA data acquisition engine can retrieve variables and status information from remote sources such as RTU, PLC, data concentrators, other supervisory systems, and protective equipment, among other sources, by the means of standard communication protocols.

The system shall be able to Monitor analog values such as Volts, Amps, Watts, energy and VARs, Pressure, volume, flow, levels, line pack, among others, at each substation. Convert these values to a digital format. Transmit changed values back to the Master Station. Convert these values into engineering units. Display these values on single line diagrams or schematics and provide alarm limit checking. Provide historical storage at user definable interval and retention periods.

The data acquisition module should not require of any protocol converter or front-end processors, all protocols should be native to the system.



The SCADA system have the capability of providing health monitoring of the host server, Ethernet switch, and terminal servers by means of SNMP, and the health monitoring points integrated into the SCADA database and accessible by the GUI.

The system can accumulate kilowatt-hour pulses from pulse initiators at each substation. Provide a freeze of counts by RTU on a user definable interval. Transmit the counts back to the Master Station. Convert the counts into interval and hourly deltas.

2.1.10. Supervisory Control

The system enforces the utilization of "Select Before Operate" (SBO) procedure that is fully compliant with IEEE Std C37-1-2007.

The system requires secure handshaking with the RTU before any controls are executed. In such cases, control of a point requires the following exchange of messages:

- Master to RTU - control point selection
- RTU to Master - point address checkback.
- Master to RTU - control execution
- RTU to Master - execute acknowledge.

If the scan task does not receive proper acknowledgement of either the select request or the execute command, a checkback failure alarm should be raised. If the acknowledgements are correct, but the expected status change does not occur within the point's control response timeout, a control failure alarm should be raised. An optional multiple status change validation feature should be available to handle cases where a control causes multiple status changes to occur.

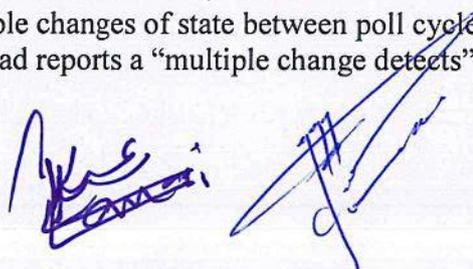
Based on noisy serial or radio communications, the system provides settings to configure the response time before control failure alarms are raised.

The system shall allow for secondary passwords on controls. The secondary password shall be defined for each user account and capable to be enabled for individual status points or system wide.

2.1.11. Communications

The software subsystem for the proposed protocols shall implement all features of the RTUs and IEDs that are required by the DPDC. As a minimum, the following functions shall be included:

- Rapid polling of RTUs for exceptions
- Select Before Operate (SBO) control execution.
- Variable control durations for momentary controls
- Detect and report multiple changes of state between poll cycles, if the RTU does not buffer changes but instead reports a "multiple change detects".



- Automatic interleaving of multiple priority messages, e.g., automatic “fast scan” after a control and “error scan” after a communication error
- Scheduled accumulator freezes and polls.
- Scheduled integrity (general interrogation) polls.
- Report by exceptions and continuous polling.
- Multiple alternate channel switch on primary error or fail detection.
- Automatic polling starts after server failover.
- Time synchronization of the RTUs
- Data exchange server and client capabilities without external modules.
- Close loop communication simulator
- Native communication protocol analyzer.
- Sequence of events data uploading and processing.
- Monitor and display communications between Master Station and field devices.

When a user-definable error retry count expires for an RTU, the system will declare the RTU failed by means of a status point and an accompanying alarm. On RTU failure, the system shall mark all points that are telemetered by the RTU as “telemetry failed”. For each point, this telemetry failed quality code shall not clear until a value is subsequently received from the point.

The user can define alternate communication ports (or IP addresses) that can be used to reach the RTUs. On a series of communication errors with an RTU, the system shall switch ports after a user-definable port retry count expires. A separate port status point for each RTU shall be maintained to indicate which port is currently being used to poll each RTU and alarms could be raised on these points as per user preferences. If the communication line is looped, it shall be possible to determine between which two RTUs a break exists by examining the values of the port status points.

For each RTU, the system will maintain communication statistics in the form of analog points that may be viewed on displays, printed in reports, or stored in historical data files. Such statistics shall include percentage of successful communication, number of timeouts and number of security errors.

2.1.12. Data Processing

The system shall provide support for multiple status changes that result from control commands. For each control point, it shall be possible to specify a list of up to 30 status points that may change because of a command. If not all the expected transitions occur within the control point response time-out, the system shall generate an alarm for the control point as well as an additional alarm for each associated point that did not undergo the expected transitions.

The system scans every analog input in the RTUs at predefined scanning intervals. Any failure to complete a scan shall be marked with a data quality flag. Also, the system shall scan each analog input every second and compare that input to the previously reported input. When the difference between these values exceeds its reporting band, the analog value shall be reported (report-by-exception).

The system can check the analog values for at least three sets of limits: warning, emergency, and reasonability. Each of these three sets of limits shall be provided with an upper limit, a lower limit and a dead band.

M. J. Cannon

C. Cannon

To allow the removal of noise readings around the zero mark of the engineering scale, a range of engineering values inside the point value range will be specified which shall clamp the input value to zero. For example, if the zero-clamp dead band is 3.0, any input value which is converted to between +3.0 and -3.0 engineering units will be clamped to zero.

The system provides a rate-of-change for analog input values by computing the difference between the new and previous value and dividing this by the difference between the current time and the time the point was last updated. The rate-of-change shall be checked against the limits for rate-of-change.

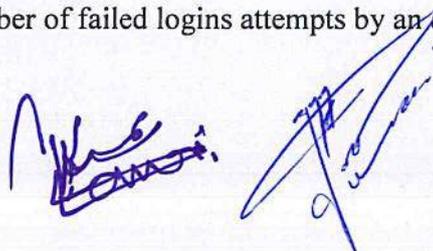
The system is to be able to process accumulators received from the RTUs. The system shall send a command to freeze the accumulators either to all RTUs or to the selected RTUs. However, this freeze command shall not reset the accumulators in the individual RTUs. Upon receiving the accumulator readings at the master station, the system shall automatically calculate the difference from the last reading. The system shall retrieve the hourly accumulators every hour from the RTUs and shall convert them to engineering units. The system shall also be able to retrieve accumulators at user-definable intervals from 15 to 30-minute intervals.

The system should be able to handle in emergency or massive disturbances at least 4,000 alarms per second peak for at least 15 minutes combining digital and analog alarms, during this period the system should handle the inbound alarms without data loss.

2.1.13. Authentication and Access Control

The system shall use username and password to be authenticated over LDAPS (Active Directory) and Two factor Authentication. A system administrator will be able to create and maintain accounts containing Username, password, Zone groups, mode of operation and the user rights for each system user.

- a) The Guest account by default restrict certain areas of the map or alarms, this account should be configurable to allow further restrictions.
- b) The system can temporarily disable a user account without deleting it.
- c) The system can deny remote access for a user account.
- d) User account passwords shall be a minimum 128-bit encrypted and neither stored nor transmitted in plaintext. The system shall allow for selection of password length greater than twelve (12) characters, and have password complexity settings for inclusion of alpha, numeric, and mixed case character requirements in the password. The system shall allow the password frequency of change to be set to 1, 30, 90, 180, or 365 days. It shall also allow setting the password to never expire. The system shall prevent the username to be part of the password.
- e) The number of upper, lower case, and special characters is configurable to enforce security. System shall prevent reuse of passwords, the inclusion of the username on the password field and, repeated strings of identical characters.
- f) The system allows a settable number of failed logins attempts by an account, and a blocked



timeout period to block the user login if the number of failed login attempts is exceeded.

- g) The system will allow for an inactivity timeout setting to be enabled, whereas after a settable amount of time of inactivity the account is logged out.
- h) Account activity logging can be configurable for login success and failures. The logging mechanisms shall be configurable for the remote Syslog protocol.
- i) The system generates and print a report of the log list that can contain information on the application used and the time accessed.
- j) Is included a Network Security Editor which defines the rules for the SCADA system to characterize TCP/IP connections.
- k) TCP connections are classified as Remote, Local or Reject.
- l) The login supports network encryption RC4 as minimum requirement.
- m) The system can support a secondary password assignable on a per-user basis. This secondary password may be required to execute control operations on some or all controllable points in the system.
- n) Each controllable point in the system supports a configuration switch to require a secondary password be entered before a control is allowed. This secondary password reduces the likelihood of an unauthorized person executing a device control.

2.1.14. User Rights

Each user account can be assigned a set of user rights that determines the actions that the user may take. This shall provide individual control over various operating and editing functions. These user rights shall include the ability to: acknowledge, block, unblock, and silence alarms; edit database, maps, reports, analog limits, and notes; manual set, control, and tag/un-tag points.

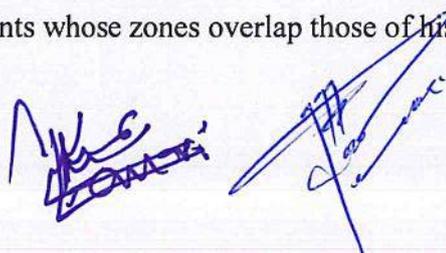
The proposed system should handle all DPDC needs in terms of number of user accounts and the corresponding user rights, required by the customers for the variety of access, profiles, and zoning access control.

2.1.15. Area of Responsibility

The SCADA software can be partitioned into 128 areas (or zones) of responsibility. The user shall have the ability to assign any combination of the 128 areas/zones to each database point (telemetered or calculated) and/or to each login account.

The user can create any number of zone groups containing various combinations of the 128 zones and to give each zone group a name.

An operator only can manipulate those points whose zones overlap those of his login account.



2.1.16. Tag Management

The system shall inhibit control of devices by means of a secure, multi-level tagging feature. This feature allows operators to apply up to eight tags to each point, each tag being stored with a date/time stamp and optional operator-entered description.

Each point displays a visual attribute showing that the point has one or more tags on each display where that point is shown. If a point is tagged, the display shall show the symbol that corresponds to the highest-level tag on the point.

It shall be possible to specify that the tag dialog remembers the last choice of action, tag type, tag number, and tag description.

The system includes the capability to configure a custom set of tag types that are mapped to the following four basic types of tags: Inhibit ON and OFF controls, Inhibit ON control only, Inhibit OFF control only, Information only (no control inhibit).

The system prevents bypassing the control inhibit caused by a tag. This applies to any and every application supplied by the vendor or written by the end user using the vendor's API.

A group tag function is provided that allows an operator to define a tag, select multiple points and apply the same tag to all selected points.

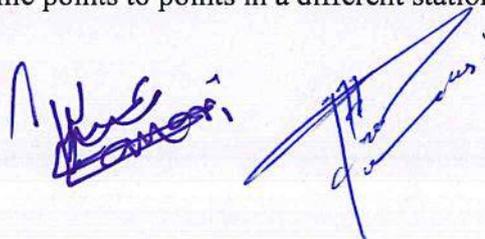
2.1.17. Database Editor

The database editor shall provide a graphical tree-like representation of the complete database and shall support easy navigation throughout the database to the desired items to be edited. Database items to be edited in this way shall include Stations, Communication Lines, Communication Channels, RTUs, IEDs, as well as all the individual database points (analog values, status indications, accumulators, etc.).

The database editor shall operate as a "client" program which communicates with a "server" program running on the host computer. However, the database editor shall be able to run on any computer that is connected to the host server via the network. With this arrangement, it shall be possible to manage the database maintenance from any suitably configured PC on the network without being necessary to go to the control room to do it.

The database editor shall include features which will make it easy to create and modify the database such as:

- Using the Station Cloning feature to create an entirely new station and all its points, based on an existing station.
- Copying, cutting, and pasting in the Windows environment
- Using a model feature to create points and other database items that are based on previously created ones.
- Using a Station Rename feature to copy a portion of an existing display, and to reassign all those dynamic points to points in a different station, all in one operation.



- Editing or modifying the database on an MS Excel spreadsheet and importing it into the system real-time database
- Deleting existing database points
- Deleting an entire station with all associated points

All changes and updates of the database shall be completed and validated while the system is in online operation. Under no circumstances shall the real-time system operation be interrupted or disturbed by the database editing and maintenance process.

2.1.18. Alarms

Alarms and operational events are continuously synchronized in real-time to the standby host server, in the case of a dual-redundant system configuration.

The proposed system shall be able to handle a minimum of 1000 alarms or events per second per operator consoles regardless of the other workload.

The system includes ten (10 +1) alarm priority levels. Alarms with priority zero (the lowest) are pre-acknowledged. Such alarms are configured to neither sound any audio alarm signals nor cause points to flash on the display.

Each priority has its own setup and properties: variables such as how they are raised and represented can be custom programmed to each independently.

For each analog point, the user can define three sets of nested upper and lower alarm limits, with a separate deadband for each limit. In addition, analog points shall be able to generate an alarm when a rate of change is exceeded, either in the increasing or decreasing direction or both. Each alarm limit shall support a separate alarm priority.

The system should be able to block both digital and analog type alarms.

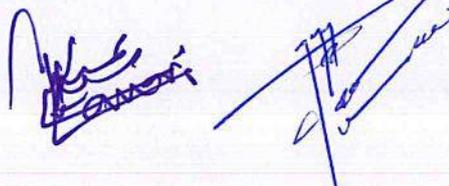
The system shall provide the operator with a visible "telemetry failure" indication when the value of any displayed point is not currently being updated by the system because of an RTU or communication line failure. Any points that are calculated using, as inputs, the values of other telemetry failed points, shall also be marked telemetry failed.

The user can specify any Windows sound file (*.WAV) to be used for the audio alarm signal. The system shall allow the user to browse for sounds and to test play the selected sounds. The system shall allow different sounds for each alarm type and a different set of sounds for each workstation.

The system provides a summary list for all unacknowledged, acknowledged, blocked, suppressed and for all alarms. The user shall be able to perform alarm filtering based on certain parameters or filters. The filtering of alarm summary lists shall be performed from a template where the operator can enter the filtering parameters and obtain the filtered lists.

2.1.19. Reports

The system shall include a report generation capability that will allow the user a high level of flexibility in the definition, formatting, and scheduling of on-demand and periodic reports. The reports shall include



data from both the real-time database and historical database. The system will allow the user to schedule reports for automatic printing or saving to hard disk files for subsequent transfer to CD or tape.

A report editor is available to allow the user to define reports by specifying a database table, a set of desired data fields and the selection criteria for retrieving records from the database table.

A graphical report in the form of scheduled prints of selected views of the world map shall also be provided.

The system packages a scheduling facility that will allow the operator to define the schedules and destinations for all reports. It shall be possible to direct a scheduled report to multiple printers, one or more of which can be directories on disk.

Reports can be exported in common formats such as PDF, XML, Excel.

Support for FTP to securely connect to or use FTP server functions using explicit SSL/TLS should be available to transfer reports on schedule. The user shall be able to define the correct certificates on server, and allow for fall-back, shall the certificate expire.

2.1.20. Data Collection and Storage

The system shall provide a historical data collection facility that allows the user to define the points that are to be sampled, the sampling frequency and how long to retain the sample data. In each dataset, the oldest samples should be overwritten by the newest.

The embedded historian will provide SCADA admin users and system operators, with reporting capabilities from the tables storing data. The end user can create reports, filters, and graphics from these historical tables.

An advanced historian shall be available as features such as real time streaming visualization, as well as historical data, on the fly creation of grids and charts, data exploration, ad-hoc queries and reporting that can be shared across the functional teams and organization. For more information, please contact your account executive.

The historical data software shall allow the user to specify the recording of statistics in the sample records. The statistics shall include time averages, summations, maximums and minimums, and times of maximums and minimums and shall be based on user-definable observation intervals.

The system shall also allow the user to create "secondary" datasets that extract information from primary datasets. For example, a primary dataset could contain 15-second samples for several days. A secondary dataset could extract daily maximums and minimums, as well as the times of the maximums and minimums and record these for ten years.

2.1.21. Data Trending

The proposed system shall provide the ability to store and view any data value from the database in a trend graphical format. The system shall bring up pixel-resolution trend graphs of historical data. Sample

rates as low as 1 second must be supported.

Trend graphs shall be displayed in separate windows that can be moved, re-sized and minimized to an icon. The trend graph window shall include tools that allow the user to configure and customize the graph display.

A trend graph window shall have the ability to plot at least ten (10) points from the historical database. The trend graph displays shall be interactive allowing the operator to quickly adjust the time frame, duration, and resolution of the graph.

In cases where there are more samples in the dataset that can be displayed in the graph window, it shall be possible to scroll back in time. It shall be possible to see the numeric values and timestamp of the traces at any time position in the graph by manipulating a time cursor inside the trend graph.

The user shall be able to display trend comparison graphs from left to right, for at least ten (10) comparison trends. In trend comparison graphs, the time origin at the extreme left of the graph is a fixed time of the day; however, it may be a different day for each trend. The purpose of this is to allow the user to observe the build-up of the current day's trace, e.g., a load curve, against that of other days in the past, typically the days that contained the last week peak or the current month peak, etc.

The trend comparison graph shall have an option to set a start time and day of the week so that the trend graph is automatically launched.

2.1.22. Graphical User Interface (GUI) Functional Requirements

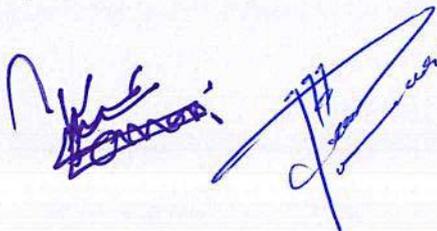
2.1.22.1. GUI

GUI for operators shall support modern graphics hardware to accomplish high-quality graphics, providing a platform for the operator to view and edit SCADA applications.

GUI shall support running OS environment of Windows 8.1 or higher and offer a tabbed interface, allowing quick access to multiple views (map, alarms, operations logs, and graphs) within a single screen.

GUI shall support:

- The ability to control/monitor any telemetered device in the field.
- Touchscreen display
- User access controls based on privileges.
- Support various GPS projection schemes.
- The capability for operators to save workspace configurations.
- Importing CAD files directly into an existing map.
- Importing GIS network topology (Requires additional software)
- Line sections to display the current state of electric or water lines (SCS license required)



- Tagging or adding notes to any device in the map
- Trace multiple and simultaneously line sections on the network topology (requires licensing)
- The ability to view Reservations when editing the map.
- Embedded control panels within maps to model field IEDs
- The capability to turn on/off the secondary network in the map.
- Separate views for Maps, Alarms & Event Logs
- The capability to view Alarms & Event Logs in the map tab.
- The capability to create and view ad-hoc or historical graphs (including 3D graphs). In ad hoc graphs, the user can view the sum of up to three points or the difference of two points.
- Provide a tabular view on trend graphics.
- Editing capabilities - create/modify/delete objects on a map.
- Diagnostic logs for fast, efficient troubleshooting
- DB points shall be able to be created from GUI when necessary privileges are enabled to the user.
- Support interfaced to AVL applications.
- Represent Distributed Energy Resources (DER) generators, these shall be able to be imported or manually edited.
- Keyboard shortcuts for common actions.

2.1.22.2. Drawing Tools

The system shall provide the capability to:

Access libraries with the following elements that can be added to a map:

▪ Fonts	▪ Symbols
▪ Symbol Tables	▪ Colors
▪ Color Tables	▪ Widgets
▪ Control Panels	▪ Templates

2.1.22.3. Group Views and Layers in a tree hierarchy.

Two handwritten signatures in blue ink are present at the bottom of the page. The signature on the left is more stylized and appears to be 'M. ...'. The signature on the right is more legible and appears to be 'C. ...'.

The system shall provide the following capability.

- a) Declutter the map using layers. Layers can be configured to only be viewed by users in a specific zone group.
- b) Define the topology of a network using line sections.
- c) Support multi-user editing and job partial or total reservation with a log of changes and users.

2.1.22.4. Notes

The system shall provide the capability to view, create, and maintain Notes in the system. Notes can be applied directly to the map or associated with a switch, transformer, or meter.

2.1.22.5. Operator Display

The system shall provide the following capability.

- a) GUI shall be capable of displaying a geographic map that shows all the distribution circuits.
- b) GUI shall have the capability to open a separate magnification window to display details while the main view remains open.
- c) Switchable devices shall have the ability to change their symbol and color based on their current state. The operator can manually change the device to any state.
- d) All switchable devices will have the ability to be operated by the user for any or all phases of the devices and record actual operation time (not current time).
- e) The map view can be configured to automatically declutter detail when zooming in and out (i.e., text annotation, secondary roads, etc.).
- f) A find tool is available to help find any element in the map (e.g., meter, transformer, switch, etc.). An Advanced Query tool is also available for more complex queries (e.g., find all normally open points that are closed and tagged).
- g) A tabular display is available that allows users to see the value of any status or analog point in the system. Alternatively, the user can only view the values of all the points that are in their abnormal state.
- h) A tabular display is available that displays all the current tags in the system with the option to find them in the map as well. A tag history table is available that display every modification or deletion to a tag.
- i) Operators could failover the SCADA host from the GUI (based on user rights).

2.1.23. SCADA Systems Applications



2.1.23.1. SCADA Historian

The Historian system shall provide the following capability.

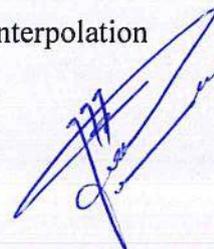
- a) The SCADA Historian will capture by exception, all point changes in the SCADA system.
- b) The SCADA Historian can also store all entries to the Operator Summary.
- c) The data in the SCADA Historian can be used by:
 - SCADA reports
 - Ad-hoc and historical graphs in the control room GUI and historical graphs in the Web Browser
 - Excel Add-In application
- d) An ODBC driver is available so that 3rd party applications can interface to the historian.
- e) A replicated historian can be installed in the DMZ as well.
- f) SCADA will support a store and forward capability if the connection to the historian is temporarily lost to prevent any data loss.
- g) A dashboarding tool is available with the historian where users can visualize the historical data.

2.1.23.2. SCADA Language

The system shall support easy-to-use high-level programming language. It shall allow the user to define and execute programs which use database points as variables. This program can be used for calculations, open-loop control or switching sequences and for closed-loop control. The program shall be started and stopped from the editor tool, or via a pushbutton menu in GUI map, or it may be triggered automatically by a status change.

This programming tool shall provide:

- Arithmetic and Boolean operators and expressions
- Circular, exponential, and logarithmic functions
- Minimum, maximum, absolute value, and modulus functions
- Delay, get time, get date functions.
- Comparison and test with branch forward or backward to labels
- Issue controls and setpoints, raise alarms and trigger reports.
- More than 52 temporary variables per program
- Arrays of constants or database points
- Comments fields
- Call other programs as subroutines.
- Two-dimensional table lookup with planar interpolation



- CPU utilization calculations per host.

2.1.23.3. Control Panel Templates

The system shall support control panel templates that graphically represent IED's within the database. The template will allow dynamic elements and database values to be superimposed over a graphic representation of the IED faceplate. The template shall support multiple pages of IED information.

The user shall be able to copy and paste a template instance on the world map, and reassign the template to a new IED, with all database values automatically updated to the new IED. When edit changes are made to the template, all instances of the template on the world map will be updated.

The user shall be able to create custom templates using the same editing tools available for editing the world map. The user shall be able to import and export templates for sharing with other system users.

The system should provide a mechanism to build custom templates or import from spreadsheets, CSV, CID or SCL files.

If an existing template is updated, the system should provide a mechanism to update all templates across the system at once.

IEC61850 Ed 1 and 2 nodes shall be supported in the Template maker tool.

The vendor shall provide in their proposal a complete list of all templates that are currently available for the system. Any associated costs for adding templates to the system will be detailed and listed as options in the price proposal.

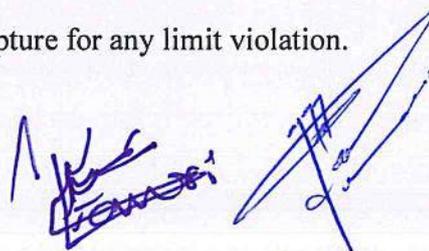
2.1.23.4. Disturbance Capture

Disturbance Capture shall allow the user to analyze the entire state of the system leading up to, and after a disturbance. All changes in analog and status points system-wide are recorded when a user-defined disturbance is detected.

Users shall be able to define the pre- and post-disturbance duration and sampling rates. The pre-disturbance duration can be set from 1 to 15 minutes, with a sampling rate of 15 seconds to 15 minutes. The post-disturbance duration can be set from 1 to 15 minutes, with a sampling rate of 5 seconds to 15 minutes. The Disturbance Capture editor allows the user to specify which points can trigger disturbance captures, and for each point, what would signal a disturbance. Points can be dragged-and-dropped into the disturbance capture settings box and right-clicked to set the state or limit.

Status can trigger a disturbance capture for a change of state.

Analog points can trigger a disturbance capture for any limit violation.

Handwritten signatures and initials in blue ink, including a signature that appears to be 'M. Jones' and another signature that is less legible.

Disturbance Capture shall keep a log of all disturbances, detailing the date and time of the disturbance, the point that triggered the disturbance, the reason code, and the recorded length pre- and post-disturbance.

There will be no limit (other than that imposed by disk space) on the number of disturbance capture files that can be accumulated.

Disturbance Capture shall include a Point Capture Viewer, which will allow users to analyze points from anywhere in the system, for a given disturbance. The Point Capture Viewer will also allow the user to select any disturbance file and export it to Microsoft Excel for further analysis.

2.1.23.5. Event Data Recording

Event Data Recording application shall provide a facility to record the following events:

- All status changes.
- All changes for selected analog points (can be calculated points)
- All control actions.
- All sequence of events (SOE) data
- All radio load shed commands.

The event data shall be stored on disk in an online data file that can contain up to 30 days of event data. The sequence of events data is time-stamped to milliseconds (subject to the capabilities of the RTU). The system shall record all logs from operators regardless of if points are enabled as EDR.

It shall be able to request reports of event data filtered by:

- Event type
- Point name (with wildcards)
- Date and time range

On command, or on schedule, online event data may be dumped into offline files for backup to tape. These files may be recovered later and reported on in the same way as for online event data.

2.1.23.6. External Alarm Bell

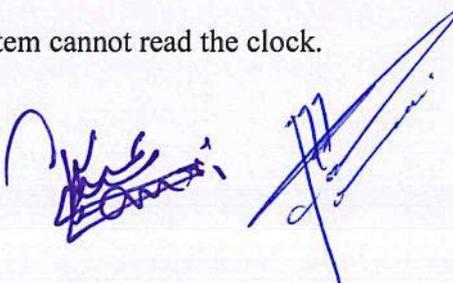
External Alarm Bell shall drive external alarm devices to be used when operating under noisy conditions or to alert personnel outside the building.

It shall be possible to define the number of external bells, and which zones they are assigned to, as well as which alarm priorities each bell will handle. Audible alarms at each GUI workstation are sounded.

2.1.23.7. External Clock Interface

External Clock Interface shall allow the SCADA master to synchronize its computer time to that of the external (GPS) clock every minute.

An alarm will be raised if the SCADA system cannot read the clock.



When outfitted with a Frequency and Time Deviation Monitor option, the clock will provide, in addition to a GPS-based reference time, the following data:

- Line frequency (in mHz)
- Frequency deviation from 60 Hz (in mHz)
- System time based online frequency.
- Accumulated time deviation (in milliseconds) between the reference time and the system time.

The system shall allow you to pre-set the time deviation to the clock. Both the frequency deviation and the time deviation points may be used as inputs to Automatic Generation Control.

The system shall support dual redundant GPS clock configuration, in case of the primary clock or communications failure.

2.1.23.8. Fault Data Recorder

The system shall support Fault Data Recorder, which will allow users to upload and record fault data from relays.

The editor shall allow users to identify fault data points as well as other points and parameters that are involved in the process of retrieving the fault data.

In a relay, fault information (such as fault current, fault type etc.) is queued and stored in a buffer inside the relay. When commanded, the relay de-queues and transfers fault data to a group of data points called Relay Summary Event Data.

A relay fault indicator point indicates the readiness of the fault event queue. The value of this status point becomes 1 if there is at least one set of unread fault data in the queue.

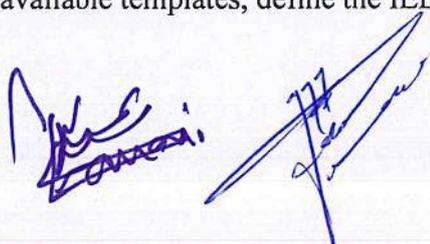
To read the fault data, the master station sends a control command to a specific binary output point of the relay. This causes the relay to de-queue the oldest fault event and load the fault data into a set of analog points. These analog points are reported to the master station in the usual way (by exception, for example, if the communication protocol is DNP). After processing the received fault data values, the master station then checks the fault indicator point again, which will still be "on" if the queue contains more unread fault event data. The master station continues this process until all the fault event data is read, whereupon the fault indicator point goes to the "off" state.

The executive program of the Fault Data Recorder can be configured to operate in either Automatic Upload mode or in Manual Upload mode.

2.1.23.9. IED Wizard Templates

The system shall support Intelligent Electronic Device (IED) wizard templates for automating the creation of points for IEDs on the system.

The user shall be able to select from a list of available templates, define the IED name, communication



line, IED address, communication statistics for total message count, good message count, and bad message count received from the IED.

The template shall contain all available points for the given IED and allow the user to select the points to be included in the database. All the telemetry and control addresses and RTU-to-IED mapping shall be automatically generated.

The Vendor shall provide an application that allows the user to create new IED templates and edit existing templates.

It shall be possible to create IED templates for IEC 61850 devices.

The vendor shall provide in their proposal a complete list of all templates that are currently available for the system. Any associated costs for adding templates to the system will be detailed and listed as options in the price proposal.

2.1.24. Inter Control Center Protocol (ICCP)

Inter Control Center Communication Protocol (ICCP) is the industry standard for Master-to-Master communications. ICCP application consists of both client and server software.

ICCP should run natively on the host server without any protocol converter or front-end processor.

The client software connects to other members on the network to request point data and forward control requests from operators and application programs.

The server software responds to client requests by returning the requested data and executing (if possible) the requested controls.

Quality codes, such as manual set and telemetry failed, are transmitted along with the data. In device control operations, tags on the server system are respected.

Any member of the ICCP network can act as either a client or a server or both. The relationship between any pair of members may be fully bidirectional. That is, both members may act as both client and server to each other. Furthermore, any member may act as a server to multiple clients, and at the same time act as a client with multiple servers. Establishment of the connections is the responsibility of the client software.

The client and server software consists of two separate programs. Every member of the network runs a separate copy of the server program for each (client) member that wants data from it.

Similarly, every member of the network also runs a separate copy of the client program for each (server) member that it wants data from. In a bidirectional link between two partners, this means that each partner runs both a client program and a server program connected to the other partner.

By defining groups of points called virtual RTUs, the system manager (the user) on each server system defines which points in his database are accessible for polling and control by other member systems on



the network. The virtual RTUs are defined using a Virtual RTU editor. A virtual RTU is a group of analog, status, accumulator, and control points.

ICCP supports conformance blocks 1, 2, and 5 and, MMS Services are supported.

SBO for setpoints should be enforced. The system supports Secure ICCP, as per IEC 62351-4 Standard.

2.1.25. Virtual RTU

Virtual RTU application allows for quick and easy setup of a virtual device that can be polled by another master station via DNP3.0, Modbus RTU, QUIN RTU, IEC 101, IEC 104, or Harris protocols. This is an alternative to ICCP for sharing data between two SCADA master stations.

The system shall support virtual RTU connection for sending data to other master stations. The virtual RTU shall support the following:

- Status
- Analog
- Accumulator
- Control
- Setpoint

The Virtual RTU editor is used to create one or more Virtual RTUs for each server. Each Virtual RTU references a Dataset of SCADA points whose values are to be reported to the client.

The Datasets editor is used to create sets of points that are referenced by the Virtual RTUs. Each dataset contains blocks of status, analog, control, setpoint, and accumulator entries to which SCADA points can be mapped.

Outbound Scaling factor should be supported.

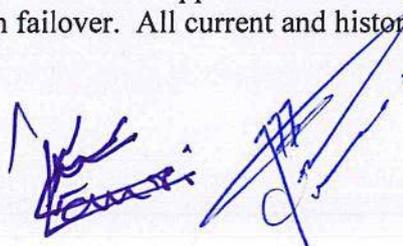
Points are easily added to the Virtual RTU with the Drag-n-Drop Point Browser.

Virtual RTU includes all the editors for setting up the communication connection and how the data is formatted when polled by the other system.

Complete Datasets can be created and assigned to multiple Virtual RTUs. This means that the same data can easily be sent to more than one master system without having to maintain duplicate dataset definitions for each Virtual RTU.

2.1.26. Interface to Microsoft Excel

The system shall support current and historical database access from clients running MS Excel. It shall be possible to directly connect to the SCADA host from within MS Excel by defining the Hostname and valid user account with username and password. The client application shall support redundant Host and automatically reconnect to the active Host upon failover. All current and historical tables and fields shall be accessible through this interface.



For current data, the user shall be able to select a database table, data fields within the table, and logic criteria (<, >, =, AND, OR) for point selection. In addition, the user shall be able to browse for points and drag-drop them into the point selection dialog. The user shall be able to select the MS Excel worksheet, start row, and start column for where the data will be populated, and to include the column headings from the database table. The user shall be able to optionally define a time interval at which the current data is automatically updated on the worksheet.

For Historical data, the user shall be able to select points contained within a historical dataset. The user shall be able to define a time type by defining the start and finish date and time, or the number of previous days, hours, and minutes. The user shall be able to select data condition codes to be included with the samples. The user shall be able to select the MS Excel worksheet, start row, and start column for where the data will be populated, and to include the column headings from the database table.

It shall be possible to save current and historical queries as defined above as reports available in the world map operator interface.

2.1.27. Master/Slave Alarm Suppression

Master/Slave Alarm Suppression allows alarms to be filtered so only the real cause of the problem is presented on the alarm display. It allows the user to define a hierarchy of primary and secondary (master/slave) alarm point relationships. These relationships may be used for Alarm Suppression, and for Group Acknowledgement.

If the alarm suppression function is enabled for a particular master/slave relationship, then as long as the master point is in the alarm state, alarms on its slave points are suppressed (i.e., the alarm severity is reduced to zero). The suppression may be specified to be either time-limited or indefinite.

If the group acknowledgment function is enabled for a particular master/slave relationship, then whenever an alarm is acknowledged on the master point, its slaves are acknowledged as well.

Each master can have any number of slaves, each slave can have any number of masters, and a slave can also be a master and have slaves of its own.

2.1.28. Network Database Access (NDA) API

The system shall support Network Database Access API (application programming interface). This is a library of functions that allow PC application programs to access the SCADA system using the NDA protocol. This API is provided in the form of a DLL (dynamically linked library) that is installed on the PC. The underlying network protocol used is TCP/IP.

The system shall allow the NDA API library (which is provided as a 32-bit DLL) to be installed on Windows PC application programs that call NDA API functions to act as clients to the SCADA system.

The system shall provide a NdaConnect function to allow a client program to connect to the SCADA system. When a connection is established, a server process is created on the SCADA system to service the client's requests. The connection is maintained until a NdaDisconnect function is called. If the connection

fails while the client application is running (e.g., because of failover), the API automatically attempts to reconnect several times. If the connection cannot be re-established, and if attempts to access the second machine of a dual master system also fail, the API returns a connection error indication to the client application.

The system shall provide the following functions for the NDA API:

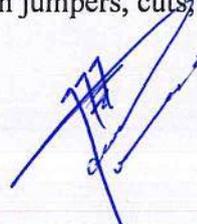
- Connect Functions. These functions allow applications to connect and disconnect from the SCADA host computer.
- Database Access Functions. These functions allow application programs to read and write selected fields from the SCADA point database.
- Control Functions. These functions allow application programs to issue control requests and monitor the results of controls.
- Alarm Functions. These functions allow application programs to read and write SCADA alarms and display fault messages to the operators.
- Error Handling Functions. This function translates NDA error codes into corresponding error message text strings.

2.1.29. Network Topology Processor

The system shall provide the following functions:

- a. The Network Topology Processor application shall automatically and constantly monitor equipment status changes and determine the current network connectivity (the “as operated” connectivity) based on the open/closed status of all system elements.
- b. The Network Topology Processor shall detect, analyze, and graphically highlight the following network conditions:
 - The energized, de-energized and/or grounded state of every element in the Distribution network
 - The line segments, nodes, and devices electrically connected to each feeder in the current state.
 - Network loops: alternative power-flow paths to devices from a single power source
 - Network parallels: multiple power sources to the same portion of the network
 - The status (normal or abnormal) of all devices
 - All devices in an abnormal state (e.g., a normally open switch currently in a closed state)
 - Ability to show adjacent feeders (circuits with open breakers or tie switches)
 - Differences in the frequency/phase at the feeder head.
 - Highlight line sections that are experiencing overvoltage, undervoltage or overcurrent
- c. NTP is an application that calculates and displays the energized/de-energized status of network line sections in the GUI. The calculation is based on the topology of the network and the status of breakers, switches, and other circuit elements. For areas that are energized, NTP also indicates where the network is paralleled or looped. When a circuit becomes de-energized, paralleled, or looped, NTP shall raise an alarm to alert the operator.
- d. The color-coding used to indicate line section status is user-defined. Multiple color-coding schemes can be used if desired (e.g., one for high voltage and one for medium voltage). Feeder-

- based color-coding is supported (circuits are colored according to which feeder they are presently connected). The user has the option of specifying which coloring they wish to use for their session – by voltage or feeder.
- e. A feeder trace function allows multiple circuits to be highlighted in different colors. Traces can be specified to be bidirectional, upstream, or downstream. The trace can be to the next protective device or the feeder. Traces can be done on de-energized line sections as well.
 - f. SCS supports independent phases in each line section. You can specify any combination of 1, 2 or 3 phases. If the line section is a switching device, you can specify whether the device is ganged or non-ganged. If ganged, specify just one SCADA point. If the device is non-ganged, then a separate SCADA point is specified for each phase.
 - g. ABC, RYB and RWB conventions are supported.
 - h. SCS performs three independent connectivity calculations, one for each phase. The second set of user-defined colors is used to represent line sections that are "partially energized".
 - i. Loops should be prevented to be calculated in normally closed ties.
 - j. Graphics representation not required to have three separate lines to represent circuits controlled by non-ganged devices. For example, in a three-phase non-ganged switch, you could place three switch symbols on the map side-by-side, and group them together into the one-line section. On either side of the switch group, you can have single three-phase lines on the map. If one phase goes down, these three-phase lines will be colored "partly energized". Any single-phase laterals for that phase will be colored "de-energized".
 - k. On the live map, line section data can be obtained by clicking on the desired line section. A line section data window appears to display the status of each phase contained in the line section and identifies the source feeder for each phase. If the selected line section is below a substation, the line section data window identifies both the upstream substation feeders and the transformer station feeders that feed the substations. If the selected line section is above the substation level, the line section data window only identifies the upstream transformer station feeders. The next upline line section will also be displayed with an option to find in map.
 - l. The line section data can also be viewed by simply placing the mouse pointer over a line section. The displayed data includes customer counts and status of each phase.
 - m. From a line section, a function is available to find the next upline or downline protective device.
 - n. From a line section, a function is available to view the installed kVA downstream of the line section.
 - o. The customer count downstream of a line section (total or by phase) can be displayed on the map.
 - p. A user cannot energize a grounded line section.
 - q. Capability to insert and remove temporary devices such jumpers, cuts, grounds, mobile generators,



and temporary switches.

- r. Manually setting the status of a temporary device will be logged in the Operator Summary.
- s. Multiple temporary cuts, jumpers, and switches should be supported on the same line section. Temporary devices should be supported in switch orders.

2.1.30. OPC Client/Server

The OPC Client/Server application includes options for both OPC Client and OPC Server to make possible interoperability between automation and control applications, field systems and devices and business/office applications.

The Master must support the OPC functions listed below. The OPC Client shall:

- Allow Scan Task to connect to a compliant OPC DA Server and receives data from the Server.
- Receive point information in the native format provided by the Server, therefore no special formatting is required.
- Support DA (Data Access) 3.0 or 2.05a connections
- Support redundant Servers.
- Support synchronous or asynchronous read/write operations.
- Allow the OPC Client to refresh all points (all data poll) periodically optionally.

2.1.31. Operations and Outage Accounting

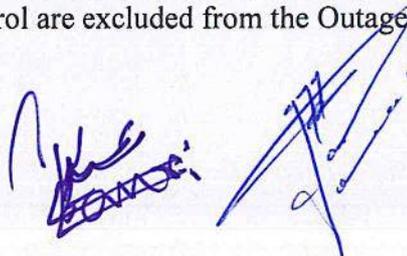
Operations and Outage Accounting makes use of controls and status change events contained in the event data recording data file.

An Equipment Editor allows you to specify the devices for which accounting is required. An Operations/Outage Accounting module, which runs every day, scans the event data file for the previous day and generates the required accounting data. Special-purpose report modules generate the Device Operations and Outage reports.

For operations accounting, the accounting module counts operations found in the event data file. Separate counts are maintained for the number of operations caused by operator control and the number of operations caused by protective relaying. The program raises an alarm for any operation counts that have reached or exceeded user-defined warning limits.

For each breaker, the Device Operations report includes the time and date of the most recent operation, the number of days elapsed since the last operation, and the number of operations (caused by operator control, caused by protective relaying, and the total).

For outage accounting, the accounting module produces a daily outage summary file. It also updates the total accumulated outage (duration) value for each breaker. Outages with durations of less than one minute and outages caused by operator control are excluded from the Outage report and from the total accumulated outage time.



For each outage, the Outage report includes the time and date of the start of the outage, the duration of the outage, and the last phase currents available immediately prior to the outage.

2.1.32. Remote Alarm Annunciation

Remote Alarm Annunciation is designed to forward the selected alarm messages to operators or other responsible personnel who are away from the control room.

The Remote Alarm Annunciation system can use any combination of the following messaging mechanisms:

- Call a central paging computer and submit a digital alphanumeric page request.
- Send e-mail, via your e-mail server.
- Send a SNMP "trap" message to a compatible network management station.
- Make a voice announcement using a voice synthesizer and the telephone network.
- Send a SMS text message to your cellular telephone.

In each case there is communication between the SCADA Master and another device, using the appropriate communication protocol.

The paging connection uses the Telelocator Alphanumeric Protocol (TAP), e-mail relies on the Simple Mail Transfer Protocol (SMTP), traps are sent using the Simple Network Management Protocol (SNMP), and text messages are sent using the Short Message Service (SMS) provided by a cellular company.

Voice messages are sent as plain text to an external speech synthesis device.

It shall be possible to assign annunciation messages to any point-related alarm (e.g., analog limit violation or unauthorized status change). The user can define a schedule for Remote Alarm Annunciation so that it becomes active automatically after business hours and deactivates automatically in the morning.

Users may also specify:

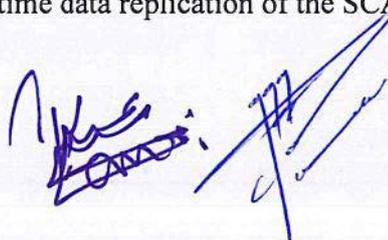
- Remote annunciation delay, the minimum delay before a remote alarm annunciation is sent on a per-point basis.
- Whether the annunciation will be sent even if the alarm has already been acknowledged on a per-point basis.
- Re-annunciation time interval, such that if the alarm is not acknowledged after this time interval, the page will be re-issued.

SMS text message alarms received may be acknowledged from their remote location if you permit it.

To acknowledge the alarm, the recipient of the annunciation message simply replies to the message with 2 numeric codes (3-4 digits) from the original alarm message, and a password that is defined for the user.

2.1.33. SCADA Replicator

SCADA Replicator application provides real-time data replication of the SCADA database to a SQL Server or Oracle database.



The editor allows the user to select any Table within the SCADA database, and from within any table, any combination of fields to be replicated. The Historical Data Sets panel contains a list of all the historical datasets that are in the SCADA system. Users can select which datasets you wish to have replicated by using the checkboxes.

Archiver, a companion program to SCADA Replicator, can be used to extend the historical data tables beyond the sizes imposed by the configuration of the SCADA system.

The Archiver does this by transferring the data from the replicated tables into a parallel set of archive tables and allowing the archive tables to grow to a much larger size, or even indefinitely.

Replicator automatically fails over to the current active SCADA host.

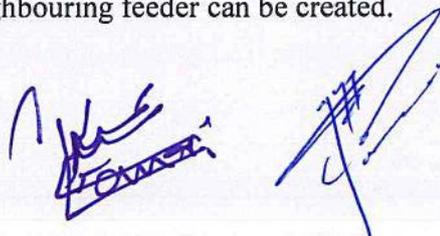
Replicator itself can be configured to be redundant. The SCADA host can support up to four concurrent dual-redundant Replicator connections.

The Archiver can be installed on multiple computers to provide multiple archiving services. Each instance of the Archiver can be configured to archive any combination of historical tables from the replicated database into another database.

2.1.34. Schematic Generator

The Schematic Generator allows operators to select a line section from their GUI and view the schematic representation of the selected feeder.

- a) The Schematic Generator can work on either the sub-transmission or distribution level.
- b) The Schematic Generator can draw the schematic representation of the entire feeder or only the 'backbone' (3-phase) portion of the feeder.
- c) Next to the schematic representation, the Schematic Generator will also show the geographic representation of the select feeder for reference.
- d) The administrator can specify the symbols to be used for each network element (e.g., switch).
- e) Switches in the schematic representation can be configured to display additional information such as measurements or customer count downstream of it.
- f) Operators can highlight an area in the schematic representation, and it will be highlighted in the main map for reference as well as the geographic cut-out of the feeder.
- g) Operators can search for a point in the schematic representation.
- h) By selecting an open tie point of a neighbouring feeder in the schematic representation, a schematic representation of the neighbouring feeder can be created.

Handwritten signatures and initials in blue ink, including a signature that appears to be 'M. Jones' and another set of initials.

- i) Operators can operate devices directly from the schematic representation and the SCADA system will be updated accordingly.

2.1.35. Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application layer protocol (part of the TCP/IP protocol suite), and the de facto standard for network management.

SNMP enables the exchange of management information between network devices in a relatively simple way, thus facilitating easy incorporation of the protocol into vendors' products.

SNMP is a widely available protocol which can enable network managers and administrators to manage network performance, find faults and assess network usage, thus allowing for future network planning.

Adding SNMP communications task to your SCADA system will make data values (status, telemetry, and text) from these network devices available in the SCADA database and on map displays and allow SCADA to generate alarms from them.

SNMP shall support the following functions:

- Polls for data objects by their Object Identifiers (OIDs). Each item may be any of the supported types: integer (signed or unsigned, 32- or 64-bit counters), time ticks, IP address, bits, or an octet (byte) string.
- Stores the returned values in analog, status or even text points in the SCADA database.
- Supports controls and setpoints via SNMP write operations.
- Each RTU may be configured individually to use SNMP v1, v2c or v3.

2.1.36. Switch Orders and Guarantees

The Switch Order and Guarantees application shall be accessed through the GUI.

- a) A switch order is a sequence of steps involving both switching operations and tags that produce conditions for which a guarantee may be issued. Each switch order can contain up to 200 steps.
- b) A user can specify if a switch order is for planned or emergency work.
- c) The administrator can specify whether the switch order sequences must be executed in order.
- d) A user can skip a switch order sequence.
- e) A switch order can be modeled so that it can be re-used.
- f) Temporary devices can be applied/inserted/enabled or removed/disabled in a switch order.
- g) Switch orders can include sequences for actions that do not have a point in the system (e.g., SPECIAL step).



- h) A user can automatically execute the entire switch order (with a pre-defined delay between each step).
- i) (If configured) The user must specify who ordered a sequence before it is executed.
- j) A restoration order can be created from a switch order where the switch order application will automatically reverse the order of the sequences and operations (e.g., open to close).
- k) Users can filter the switch order list by time, switch order type (planned or emergency), switch order or restoration order, status of the switch order,
- l) Guarantees are forms that describe a set of tags. They may be used standalone or in association with switch orders. Tags in a guarantee that has been issued cannot be removed until the guarantee has been surrendered. (Hence the name guarantee – the form guarantees that the tags will remain in place until the guarantee is surrendered.) A restoration order that has a guarantee associated with it cannot be executed until the guarantee has been surrendered.

2.1.37. Browser

2.1.37.1. Web Interface

- a) Web Interface shall provide real-time SCADA information to users via a web browser, without the need for custom installation or maintenance.
- b) Web Interface allows the user to call up and view any GUI display, substation one-line, or tabular display. Refresh of dynamic data, alarms, and graphics can be user-defined and achieved on a periodic basis every few seconds. Users can access reports, graphs, and point setting information in an Explorer type interface.
- c) Web Interface uses HTML5, Silverlight or SVG (depending on browser capability) to render dynamic GUI graphics in the users' web browser, and supports panning, zooming, dynamic line coloring and other dynamic features of the GUI interface.
- d) By making use of SCADA Replicator, web server reproduces the SCADA database on a separate server thereby offloading the SCADA host(s).
- e) Web Interface is an instant, out-of-the-box solution providing unparalleled ease of use and service for your information requirements.
- f) Web Interface leverages your significant investment in GUI graphics by allowing the users to view the screens in a web browser.
- g) The Network Topology Processor shall be executed automatically in response to changes in the state of a network device that alters the connectivity of the network.
- h) The Network Topology Processor shall successfully execute for radial, networked and loop- type connectivity and shall be able to identify those parts of the network that are de-energized for a particular network state.
- i) The information provided by this application is used in the to highlight each individual feeder in the network by a distinctive color or SCADA depending on their energized and de-energized state as configured by the system administrator or selected by the operators.
- j) This application shall maintain a list of all equipment that is not in its normal state, i.e., a normally closed switch in an open state and transformers temporarily fed from

[Handwritten signature]
COMPOS

[Handwritten signature]
7/7

another phase. This list shall also include any temporary devices such as jumpers, cuts, and grounds, mobile generators, and transformers.

- k) The Network Topology Processor shall be able to detect an islanding condition and to process each individual topology as an electrically connected island.
- l) Web Interface must support:
 - A drill-down interface to view configuration and information.
 - Tabular and graphical displays
 - A common pre-configured interface
 - Automatic data retrieval from an alternate Master during a fail-over condition
 - Password protection
 - Non-control for all users.

2.1.37.2. Mobile Application

- a) Mobile Applications provides operational and control room information optimized and secured for mobile devices. Mobile Applications leverages the web server infrastructure to provide tabular and graphical data for mobile devices running Apple iOS Android, Windows, and Blackberry operating systems. The new simplified system of menus requires less memory and performs faster on mobile devices.
- b) Tabular data is available for mobile devices running Apple iOS, Android, Windows, and Blackberry operating systems.
- c) Graphical data is available for mobile devices supporting HTML5 and SVG - Apple iOS V5+, Android V3+, and Blackberry V6+ operating systems.
- d) Mobile Application must support:
 - Secure Access
 - Session Expiration
 - HTTPS for Username and Password for Login
 - Built-In Reports
 - Optimized Menu Level Access
 - Seamless, Intuitive Navigation
 - Control Panel Display Optimization
 - Administrative Tools to Manage User Accounts
 - Direct Web Page, PDF File Loading Capability
 - Portrait/Landscape Screen Scaling Optimization

2.1.38. Operator Training Simulator (OTS)

The OTS system provides facilities that allow the instructor to maintain many different copies of the database (called a 'study') and to select any of these to use for a training session. New studies can be created by modifying other studies, or by modifying a snapshot of the current real-time database.

A scripting tool is provided that allows the instructor to define and operate scripts. These scripts can be used to create sequences of events for students to react to. Multiple scripts can be initiated for

simultaneous execution. An OTS control panel window, which the instructor can invoke on any of the SCADA system's workstations, allows the instructor to initiate and manage a training session:

- Load and save studies.
- Start and stop scripts.
- Start and stop the OTS system.

The instructor can share the workstation with the student, or if extra workstations are available, there can be multiple students, and each can have his/her own workstation.

When connected to an OTS system, the GUI distinguishes itself from a real-time connection by the following:

- The title bar contains the words "OTS MODE"
- The status bar is colored bright yellow.
- In addition, the point control dialogs are further distinguished by yellow highlights around the pushbuttons. Other applications like the database editor or server manager will also have their applications highlighted in yellow to let users know they are working in an OTS environment.
- By default, the OTS GUI connects to the OTS Master on a different port than the production GUI connects to the production Master.

2.1.39. Offline Editing System (OES)

An offline editing system will be available to allow users to make and verify their edits in an offline environment before publishing it to the online production system.

Upon initialization of the offline editing system, users will be able to synchronize the OES' database with the production database to ensure that editors are editing the most up-to-date database and will not cause any conflicts when publishing to production.

Inside the OES, users will be able to create projects to do their database, graphics, and network topology edits. There can be multiple projects active at once and multiple users can work on the same project.

Changes made in a project are only sent to the production system when the project is published. Once the project is published, no more edits can be made with this project.

Users will be able to reserve any graphics file that they are working on until the end of the project. Any database point will be automatically reserved as part of the project once it is edited.

A record of all database edits and graphics files modified will be kept for each project.

There will be user rights to control who can synchronize with the production database and who can publish projects.

Depending on the type of project selected (a combination of database, graphics, or network topology edits), a visual workflow dialog will be available to walk the user through the steps required to publish the project.

In the OES, users will be able to either simulate the communication lines or start a scan task to test or use



communication lines.

Users will be able to preview what changes were made in a project before publishing the project.

All workstations will be notified whenever there are new graphic changes to download.

When connected to an OES system, the GUI distinguishes itself from a real-time connection by the following:

- The title bar contains the words "OES MODE"
- The status bar is colored different.
- In addition, the point control dialogs are further distinguished by colored highlights around the pushbuttons.
- Other applications like the database editor or server manager will also have their applications highlighted in green to let users know they are working in an OES environment.

2.1.40. Quality Assurance System (QAS) Environment

In the QAS environment, users will be able to replicate their entire production environment (servers and applications) in an offline environment that allows users to test hardware firmware updates, operating system patches, software upgrades, updates, and hotfixes. Full regression tests are performed in the staging environment prior to updating the production, offline editing, and training environments to ensure all implementation steps and procedures are accurate.

When connected to a QAS system, the GUI distinguishes itself from a real-time connection by the following:

- The title bar contains the words "QAS MODE"
- The status bar is colored different.
- In addition, the point control dialogs are further distinguished by colored highlights around the pushbuttons.
- Other applications like the database editor or server manager will also have their applications highlighted in blue to let users know they are working in a QAS environment.

Service Line Agreement: 1 year at least

Engineering Training:

Full feature training on SCADA it is recommended for FAT to be done during training:

- Installation
- DATABASE Configuration
- Graphic Design
- Command Processing
- Command Sequence
- Syntax
- Commissioning
- Test
- Project work



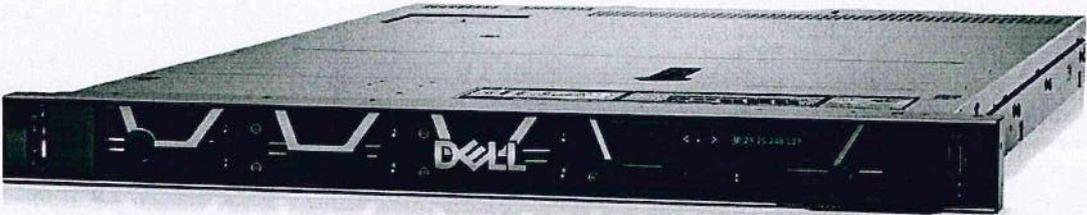
1.2 Servers + Rack Mount Monitors,

Quantity: as below

Servers are used for SCADA Platforms to be installed and engineered on it. The servers are responsible to receive site data and transmit it to the workstations for Grid Monitoring and Control.

The server shall be the most new version of Rack mount version DELL or HP Servers. It is to mention that the SCADA Platform Manufacturer cans also specify the Technical Parameter of the Server Hardware.

NUMBER	ITEM	SPECIFICATION	QUANTITY
1	Server	<ul style="list-style-type: none">- Rack Mount Server,- 2 x Intel Xeon Silver 4310 2.10 Ghz,- Dual Rank 64GB RDIMM,- At least 2TB Storage HDDs.- Redundant Power Supply,- Must have 8x Ethernet ports cards- Chassis Up To 8 X 3.5" HDD- + 2 years Extended Warranty	2PCs/Lot Total 6PCs
2	Server Monitor	19' rack mount monitor system.	1PC



Amir

Warranty: at least 2 years warranty.

M. Hassan

1.3 NLCC Workstations + Monitors and Accessories

Quantity: as below

Workstations are used for SCADA Platforms to be installed and Engineered on it. The workstations receive data from server for Grid Monitoring and Control.

The devices shall full fill all requirement included in this document. It is to mention that Workstation is designed for special operation purpose. Contractor must only supply Workstation not desktop PC.

NUMBER	ITEM	SPECIFICATION	QUANTITY
1	Workstation	<ul style="list-style-type: none"> - Workstation Tower, - Intel Xeon Silver4208 2.1GHz, - 16GB DDR4 RAM - 1TB 7200 SataHard Drive - 9.5 DVDWR 1st ODD, - Windows 10Pro, - Must Have at least 2x Ethernet ports and 2x HDMI Graphic ports - SD Card Reader, - Remote Graphics SW - mouse and keyboard, - + 2 years Extended Warranty, 	1PCs/Lot Total 7Pcs
2	Workstation Monitors	<ul style="list-style-type: none"> - Diagonal Size 27" Resolution - Refresh Rate Full HD (1080p) 1920 x 1080 at 165 Hz - Adaptive Sync NVIDIA® G-SYNC® Compatible Certified - AMD FreeSync™ Premium Technology Response Time 1 ms (gray-to-gray) - Ports 2 x HDMI, Headphones 	2PCs/Lot Total 14PCs

Amir



Warranty: Workstations and Monitors shall have at least 2 years warranty.

Mus

1.4 SWITCH

Quantity: 3 PCS

NUMBER	ITEM	DESCRIPTIONS
1	Manufacturer:	Cisco catalyst 3850 Ethernet Switch
2	Product ID:	
3	Product Description:	Cisco Catalyst 3850 Plus 48 10/100 1000BT +2 SFP LAN Lite
4	Total Number of Network Ports:	48
5	Number of (RJ-45) Ports:	48 port for connection to servers and computers
6	Ethernet Technology:	Gigabit Ethernet, 10/100Base-TX
7	Number of SFP Slots:	2
8	Management:	<ul style="list-style-type: none"> Flash 2 GB (4 GB on 12-port and 24-port SFP+ models, 8 GB on 48-port SFP+ model) VLAN IDs 4,000 Total Switched Virtual Interfaces (SVIs) 1,000 Jumbo frame 9198 bytes Total routed ports per 3850 stack 208
9	Input Voltage:	220V AC
10	Dimension(H*W*D)	(1.75 x 17.5 x 20.1) inches
11	Switch installation type	Rack mountable

Cisco Catalyst 3850 Stackable 48-Port Switch

Cisco Catalyst 3850 Switches with LAN Base Software



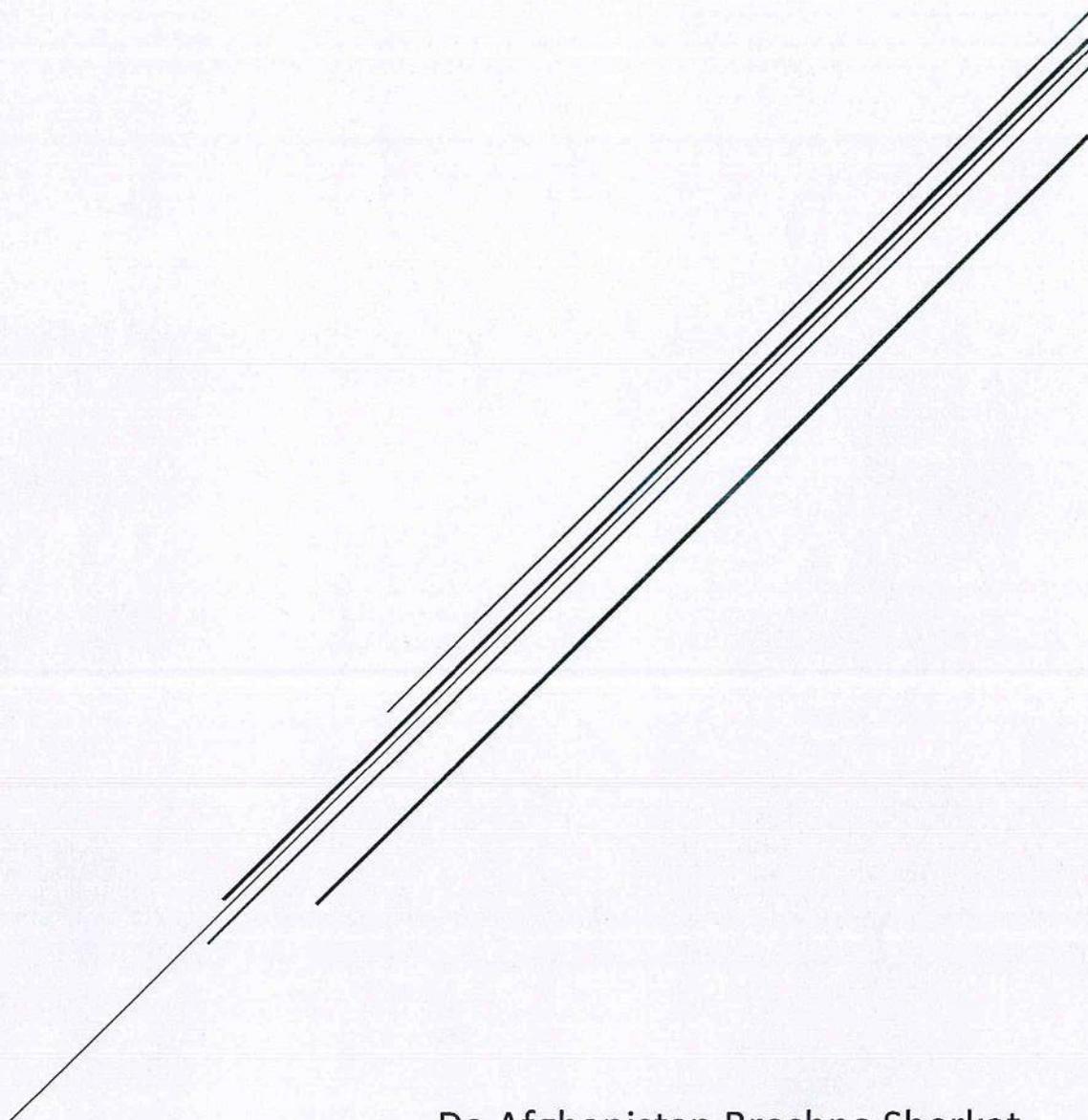
Warranty: 2 Years






SECTION 2

RTU



Da Afghanistan Breshna Sherkat
SCADA Department

2.1 RTU +Panel +Aux Relays+ Engineering Training

A- RTU

Quantity: 1 Set/Lot (Total 12 Set)

RTUs are used in almost all stations and substations SCADA systems of Afghanistan and proven to work fine and DABS SCADA team can maintain the System properly. It collects field information and send it to Control Centers inside facility and National Load Control Center. The device shall fulfill all requirements included in this document.

RTU shall be pre-installed inside Panel and its associated Connectors, cable and shall be pre-terminated to terminal Blocks at rear Side of panel.

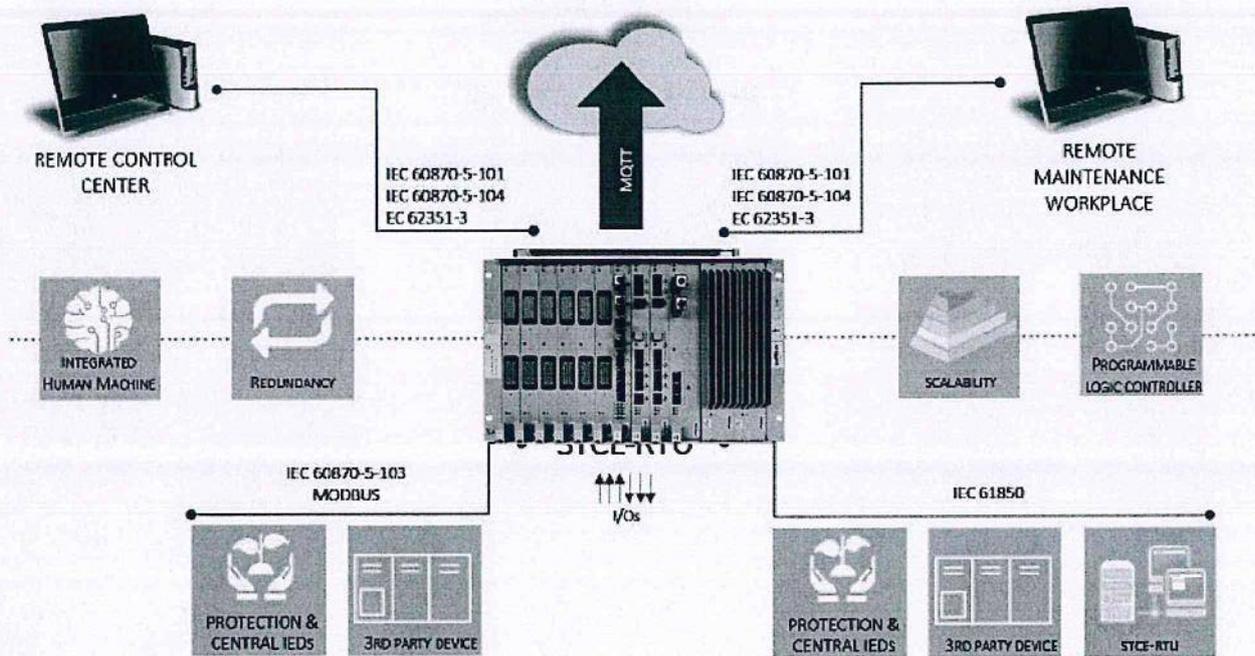
Manufacturers shall have at least 40 years' experience in remote control systems. Only RTU from International Manufacturers SEL,ABB,SELTA with at least 10 years warranty from manufacturer side shall be supplied. DABS has the right to reject any supplied item not fulfilling the requirements. **FAT test shall be conducted during the training.**

NO	ITEMS	PARAMETER
1	RTU frame and core Modules	19 inches rack mount mainframe with Core Modules, sub frame shall be include If the requirement is not full filled with only mainframe.
2	CPU	• Full license for Protocols and I/Os, at least 2 Ethernet ports and 4 Comports.
3	RTU to control centers communication card	IEC 60870-5-104, at least 4 control centers using the protocol.
4	Redundant Power supply	48VDC
5	Digital Input (DI) cards	128 DI 48VDC card
6	Digital Output (DCO) cards	32 DCO 48VDC card
7	Analog Input (AI) cards	at Least 10 Analog input Signals
8	Communication Cards to Analyzers and Relays	Modbus TCP/IP, Modbus Serial and IEC 61850 Cards/Ports with related Serial and Ethernet ports
9	Engineering Software with license and Engineering manuals for software and hardware	Configuration software with full license and manuals,
10	RTU Type	Modular
11	Connectors and Cables	Associated connectors and cables from RTU to Terminal Blocks at back of Panel.
12	SYNCHRONISM	External NTP v4 server shall be included

Handwritten signature/initials

Handwritten signature

Handwritten signature



RTU Warranty:

A letter from manufacturer addressing DABS for Warranty period of at least 10 years, Contractor is responsible for 2 years, after That DABS shall directly contact the Manufacturer.

Abbreviations:

RTU: Remote Terminal Unit I/O: Input/output DI: Digital Input DO: Digital Output
 AI: Analog Input SU: Service Unit DCO: Digital Command Output

B- Panel

Quantity : 1 set/Lot (Total 12 Set)

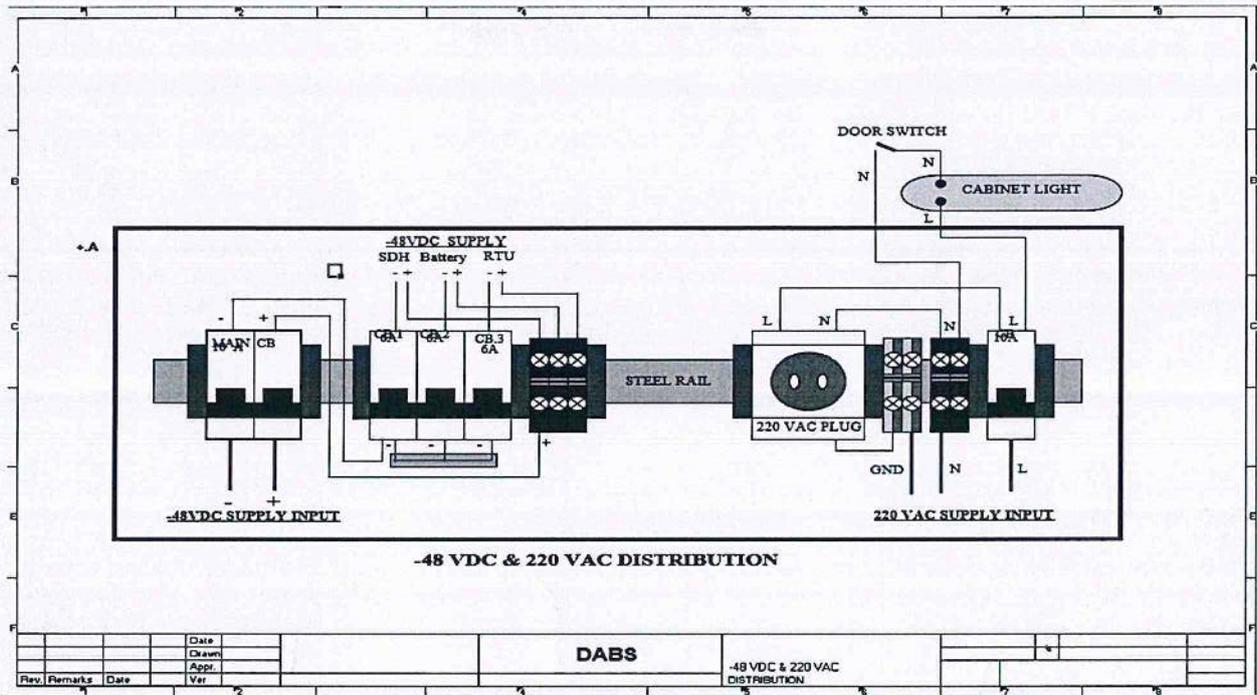
Panel shall be designed based on the requirement for holding 19" rack mount Automation, Communication Devices.

Each panel must include all the items included in this document,

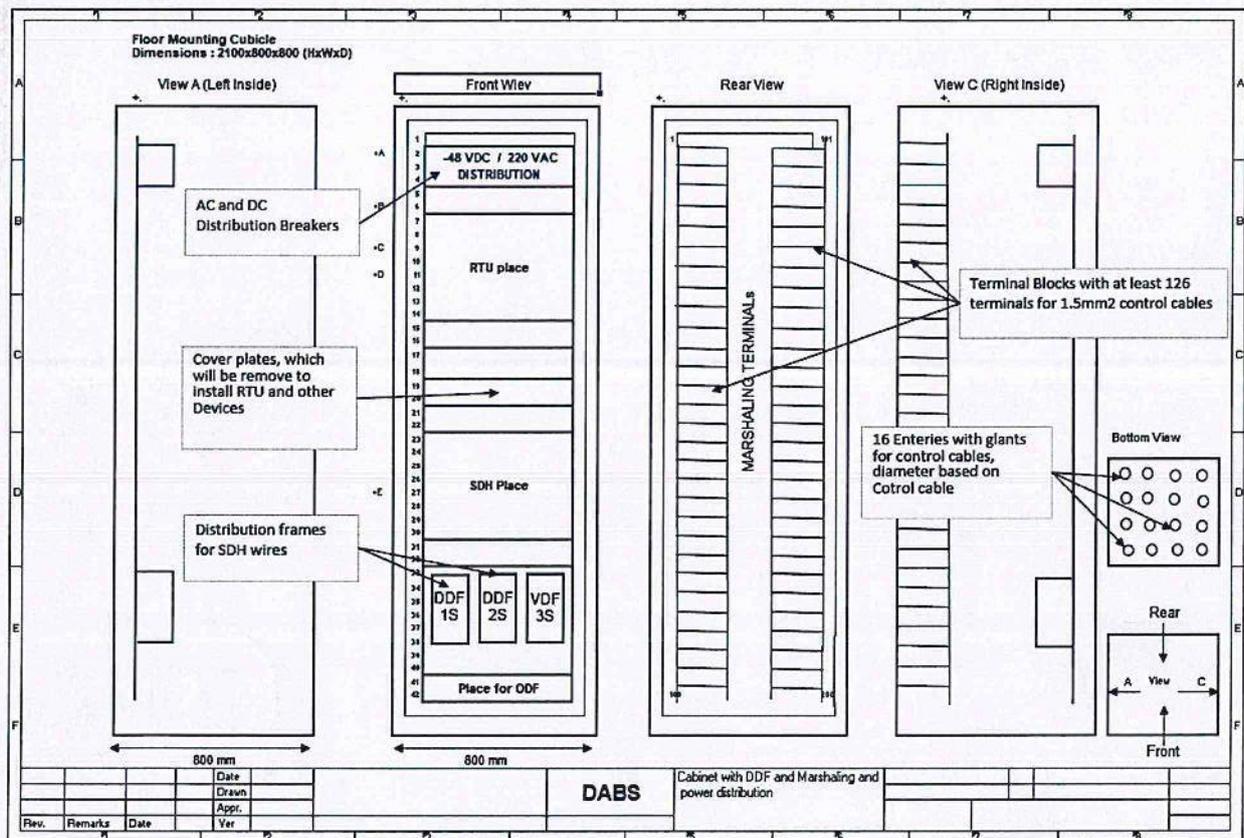
- At Front side DC and AC system and breakers must be included and pre-installed for both panels.
- At Rear of RTU&SDH panel Terminal Blocks with at least 200 terminals for 1.5mm² control wires must be include and pre-installed.
- Front of panels shall have cover plates to prevent dust inside, and space to install extra items.
- The panel must be equipped with Lockable frond door and rear door.
- Panel shall be equipped with proper cooling fan to prevent devices overheating.
- At bottom of panels at least 16 entries with glands.
- DDF shall be include and Pre-installed with panel.

[Handwritten signatures in blue ink]

Drawings AC and DC distribution System for each panel:



Drawing for RTU panel:

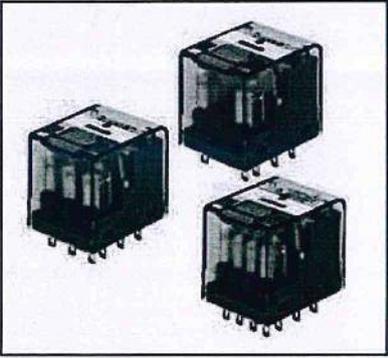


Handwritten signatures and initials:
 [Signature]
 [Signature]
 [Initials]

D- Aux Relays

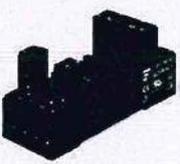
Quantity: as below

1- MINIATURE RELAY PT

Number	Item	Quantity	Parameter	Requirement
	Plug-in Relay 14 pin 4 C/O 48/110/220VDC 6A	384 Pcs 110VDC, 384 Pcs 48VDC, 1152 Pcs 220VDC Total 1920Pcs	CONTACT DATA	PT5
			Switching contacts	4 CO
			Contact style	single contact
			Type of disconnection	Micro-switch
			Rated current	6A
			Max. breaking capacity AC	1500 VA
			Making capacity, max 20	12A
			contact material	AgNi90/10 hard gold-plated
			Coil Data	
			Rated voltage range DC Coil	48/110/220VDC

2- YPT DIN RAIL MOUNT WITH SCREW TERMINALS

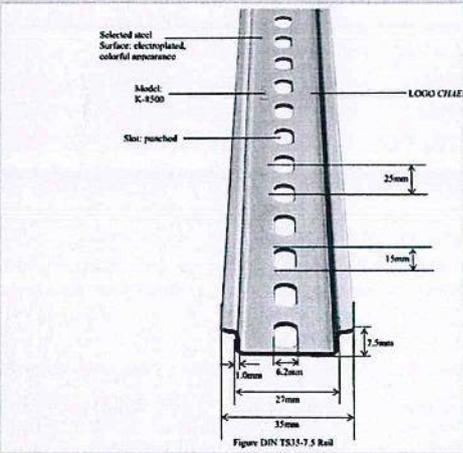
Quantity: as Below

Number	Item	Quantity	Parameter	Requirement	
 YPT7R704	ypt din rail mount Clamp	1920 pcs	Technical Data	4-POLE	
			Rated current	6A	
			Dielectric strength Coil/contact set	2500 Veff	
			Open contact adjacent contacts	1200 Veff	
				2000 Veff	
			Terminals	Screw terminals	
			Terminal capacity wire	Copper	2 x 2.5 mm ²
			Stranded wire		2 x 2.5 mm ²
			with ferrule (DIN)		2 x 1.5 mm ²

Handwritten signature

Handwritten signature

3- DIN Mounting Rail
Quantity: As Below

NUMBER	ITEM	QUANTITY	PARAMETER	REQUIREMENT
	Din Mounting Rail	192Pcs	grade	steel
			Head width	35mm
			Rail height	7.5mm
			Bottom Width	27
			Thickness	1.0mm
			Tolerance	±5%
			Length	1 meter each

Aux Relays Warranty: at least 1 year

E- Engineering Training

Engineering Training for

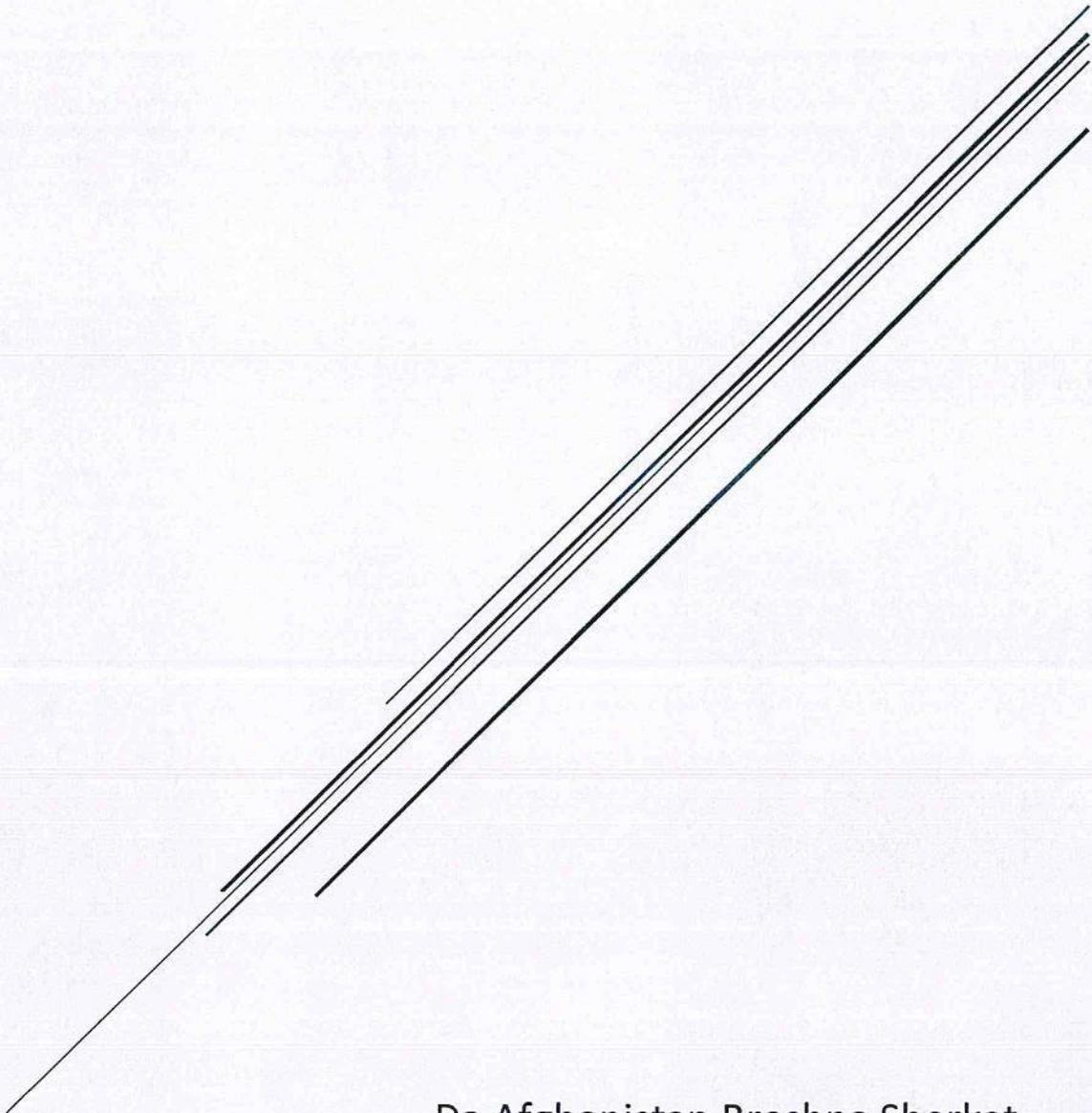
- at least 3 DABS SCADA engineers
- outside Afghanistan.
- Training Material hardware and software shall be available by the contractor.
- The training shall cover all engineering tasks
- protocols configurations,
- IO configurations,
- Installation
- Commissioning.
- Test

(Handwritten signature)

(Handwritten signature)

SECTION 3

Telecom



Da Afghanistan Breshna Sherkat
SCADA Department

3.1 SDH + Engineering Training

A- SDH

Quantity: 1PC/Lot (Total 12PCs)

Optical Multiplexer Device is used for connection of sites through fiber optic network. The SDH device shall full fill all requirement and parts included in this document.

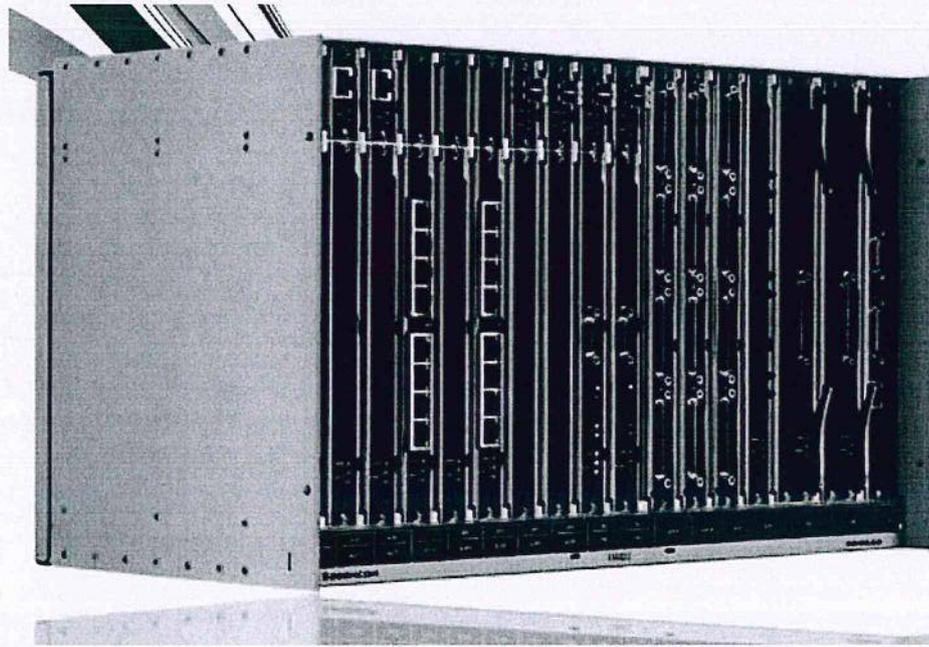
SDH shall be pre install inside RTU & SDH panel Drawing, included cable and Connectors shall be pre terminated to ODF and DDF inside panel.

SDH device supplied shall be able to connect and interface with IONOS NMS or its dedicated NMS software shall be included.

NUMBER	DESCRIPTION	QUANTITY/PARAMETER
1	SDH Equipment 19" rack mount Frame and Core Modules	1
2	Redundant common control unit, power supply, switching unit with full licenses	1
3	4X STM-1 optic port card	4
4	STM-1 SFP 1310nm 30km LC UPC	4
5	21E1 Ports card	1
6	8X port Ethernet cards	At least 3 Cards each 8port
7	Dedicated Power cable, SDH ports Connectors and cables.	Lot
8	Support MPLS-TP	A
9	Support MSTP 1+1 at least	A
10	SDH TYPE Modular	A
11	Configuration Software with License,	1
12	Engineering manuals for Software and hardware	1
13	Dimensions	6U, 19" and ETSI subracks
14	POWER SUPPLY	-48 V DC (-36 v to -72 v)
15	Matrix	16 VC4 non blocking cross-Connect at VC12, VC3 and VC4 level
16	Protections	Line Protection, SNCP
17	Ethernet features	Layer 2 Ethernet Switch VCAT and LCAS protocols, Customer VLAN and Provider VLAN support

[Handwritten signature]

[Handwritten signature]



Warranty

With at least 2 years warranty.

Abbreviations:

MSTP	Multiplexer Section Protection
SDH	Synchronous Digital Hierarchy
Nm	Nano Meter
MPLS-TP	Multi-Protocol Label Switching – Transport Profile
LC	Large Connector
UPC	Ultra Physical Contact
SFP	Small form-factor pluggable

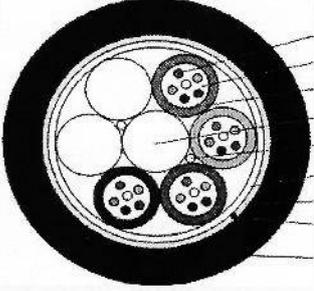
B- Engineering Training:

Training shall be conduct for:

- For at least 3 SCADA engineers
- Installation
- Configuration software and hardware
- Commissioning
- Test

3.2 ADSS

ADSS and its related fitting along with JointBox shall fulfill all requirements included in this document, the overall package include any necessary items to completely work and install the fiber system along 50m span Circular and rectangular MV poles without need for any extra items. The diameter for MV poles are 220-300 mm range at top of pole. The bracket and its related holder shall be adjustable and flexible within above range for rectangular and circular concrete poles.

NO	PIC.	MODE NO.	DESCRIPTION	QTY	UNIT
1		ADSS	<ul style="list-style-type: none"> - 48 cores ADSS, - 50m span - Single HDPE Jacket - waterproof tape - 2 pcs of rip cords - cable diameter: 9.5 - 4KM/drum 	60	KM

3.3 ADSS Suspension Fittings

NO	PIC.	MODE NO.	DESCRIPTION	QTY	UNIT
2	Refer to drawing	Suspension fitting for pole	<ul style="list-style-type: none"> - Suspension clamps for - 50m span ADSS, - with related parts included in the drawing 	2000	PCS

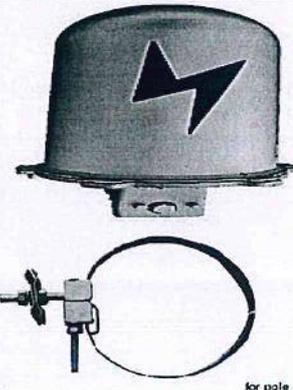
3.4 ADSS Double Tension

NO	PIC.	MODE NO.	DESCRIPTION	QTY	UNIT
3	Refer to drawing	Tension fitting for pole	<ul style="list-style-type: none"> - Tension clamps for - 50m span ADSS, - with related parts included in the drawing 	200	PCS

Parvath

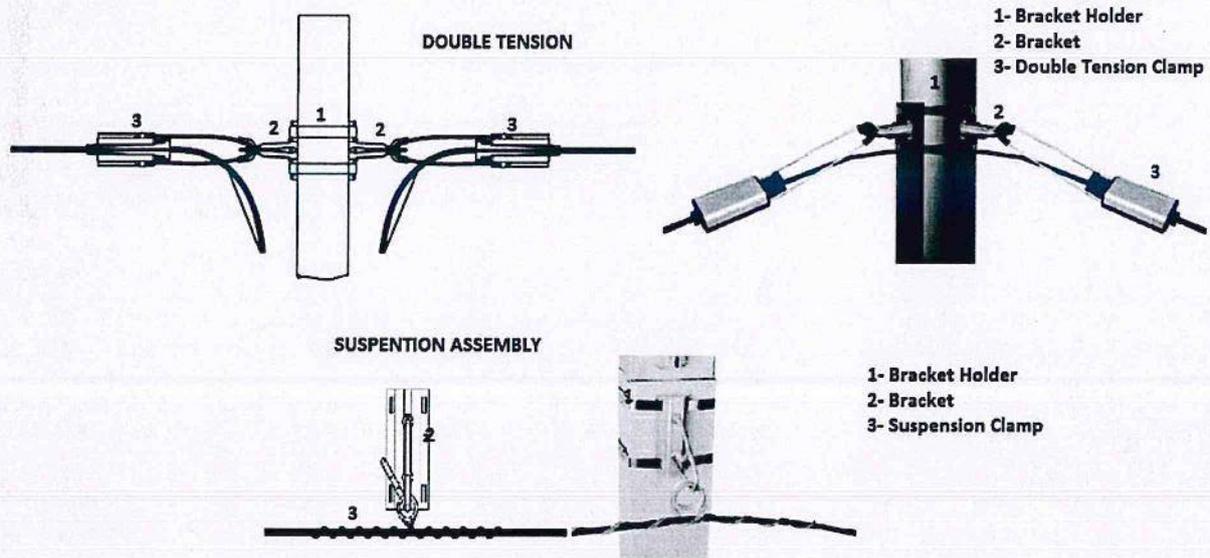
77
C. S. S.

3.5 Outdoor pole mount JointBox

NO	PIC.	MODE NO.	DESCRIPTION	QTY	UNIT
4		Jointbox for pole	<ul style="list-style-type: none"> - 2 inlet, 48core, for ADSS pole mount, - with protection sleeves, - waterproof, - with related pole mount holder and bracket 	30	PCS

Drawings

All the items include in this drawing shall be supplied to fully install the fiber optic systems.



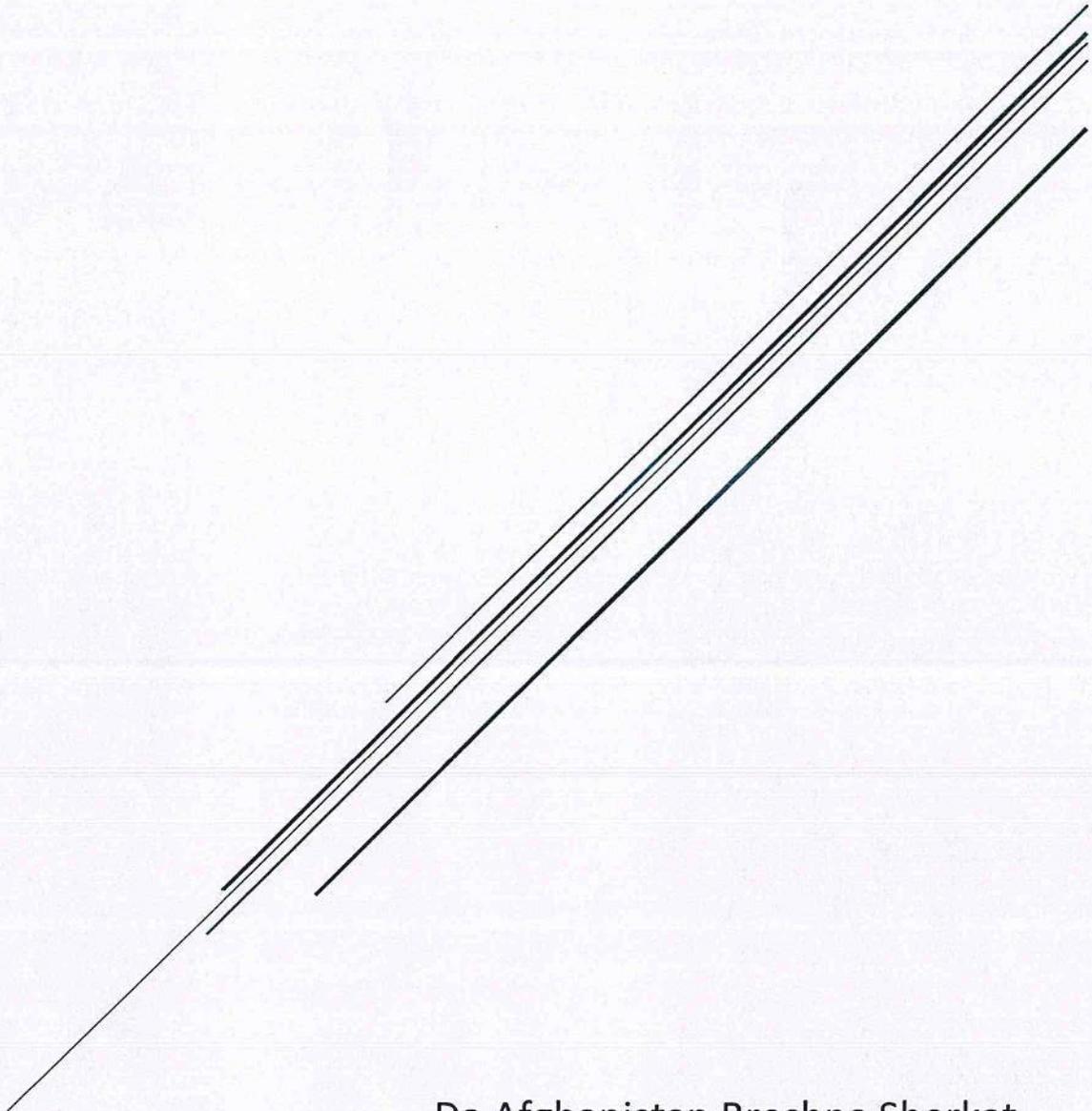
Warranty: at least 1 years

[Handwritten signature]

[Handwritten signature]

SECTION 4

HMI



Da Afghanistan Breshna Sherkat
SCADA Department

4.1 Substation Zenon HMI + Workstation + Monitor and accessories

A- Substation Zenon HMI

Quantity: 12 RT Packages and 1 Editor Package with Software and licenses

SCADA systems are world's new technology, which controls infrastructures in small scales and bigger scales like country Power Grid control and Monitoring.

Required licenses Package for the Substation SCADA System shall provide ability of direct Control and Monitoring connection to IEDs and also Trends and Alarms shall be part of the functionalities,

The license Package shall include required Dongle, serial Key, Activation Key, CDs or any other dependencies to completely work and start the Zenon Supervisor platform without any issue for lifetime.

01 ZSE12-SU-8000

zenon SE SU 8000 Tags

With zenon Service Engine - Supervisor you can visualize, control and optimize complex production plants. It is platform-independent and easy to integrate into existing plants. It converts production data into information. With more than 300 supported communication protocols, the zenon Service Engine - Supervisor connects natively with almost any existing automation and control infrastructure. The zenon network technology with seamless redundancy and circular redundancy guarantees full data security, maximum availability without downtimes and no loss of your valuable production data. You will be informed about what has happened in as much detail as you wish and will retain control over your production equipment thanks to excellent transparency.

The license should be for lifetime.

02 ZS12-DRV-IEC61850

IEC 61850 driver

The communication between driver and IED is based on the IEC 61850 protocol, using server client services via TCP/IP (profile A1/T1). The driver acts as Client during communication. The driver supports IEC time stamping and IED Quality. The IEC 61850 driver is TÜV-SÜD (edition 2) certified.

03 ZS12-DRV-MODBUS_E

Modbus Energy driver

Open Modbus TCP/IP driver with the following differences compared to the standard Modbus driver (Included in Server license):

Paula

[Signature]

04 ZS12-DRV-IEC870

IEC 60870-5-101_104 driver

Driver for the IEC 60870-5-101 (serial) and the IEC 60870-5-104 (TCP/IP) protocol.

B- Substation Workstations + Monitors and Accessories
Quantity: As Below

Workstations are used for SCADA Platforms to be installed and Engineered on it. The workstations receive data from server for Grid Monitoring and Control.

The devices shall full fill all requirement included in this document. It is to mention that Workstation is designed for special operation purpose. Contractor must only supply Workstation not desktop PC.

NUMBER	ITEM	SPECIFICATION	QUANTITY
1	Workstation	<ul style="list-style-type: none"> - Workstation Tower, - Intel Xeon Silver4208 2.1GHz, - 16GB DDR4 RAM - 1TB 7200 SataHard Drive - 9.5 DVDWR 1st ODD, - Windows 10Pro, - Must Have at least 2x Ethernet ports - 2x HDMI Graphic ports - SD Card Reader, - Remote Graphics SW - mouse and keyboard, - + 2 years Extended Warranty, 	12
2	Workstation Monitors	<ul style="list-style-type: none"> - Diagonal Size 27" Resolution - Refresh Rate Full HD (1080p) 1920 x 1080 at 165 Hz - Adaptive Sync NVIDIA® G-SYNC® Compatible Certified - AMD FreeSync™ Premium Technology Response Time 1 ms (gray-to-gray) - Ports 2 x HDMI, Headphones 	24

Warranty: Workstations and Monitors shall have at least 2 years warranty.

4.2 Junction Zenon HMI + Workstation + Monitor and accessories

A- Junction Zenon HMI

Quantity: 10 RT Packages and 1 Editor Package Softwares and licenses

SCADA systems are world's new technology, which controls infrastructures in small scales and bigger scales like country Power Grid control and Monitoring.

Required licenses Package for the Substation SCADA System shall provide ability of direct Control and Monitoring connection to IEDs and also Trends and Alarms shall be part of the functionalities,

The license Package shall include required Dongle, serial Key, Activation Key, CDs or any other dependencies to completely work and start the Zenon Supervisor platform whiteout any issue for lifetime.

01 ZSE12-SU-2048

zenon SE SU 2048 Tags

With zenon Service Engine - Supervisor you can visualize, control and optimize complex production plants. It is platform-independent and easy to integrate into existing plants. It converts production data into information. With more than 300 supported communication protocols, the zenon Service Engine - Supervisor connects natively with almost any existing automation and control infrastructure. The zenon network technology with seamless redundancy and circular redundancy guarantees full data security, maximum availability without downtimes and no loss of your valuable production data. You will be informed about what has happened in as much detail as you wish and will retain control over your production equipment thanks to excellent transparency.

The license should be for lifetime.

02 ZS12-DRV-IEC61850

IEC 61850 driver

The communication between driver and IED is based on the IEC 61850 protocol, using server client services via TCP/IP (profile A1/T1). The driver acts as Client during communication. The driver supports IEC time stamping and IED Quality. The IEC 61850 driver is TÜV-SÜD (edition 2) certified.

03 ZS12-DRV-MODBUS_E

Modbus Energy driver

Open Modbus TCP/IP driver with the following differences compared to the standard Modbus driver (Included in Server license):

- channel bundling
- improved communication with gateways
- read and write only for holding register

M. K. K.

7/17
C. K.

04 ZS12-DRV-IEC870

IEC 60870-5-101_104 driver

Driver for the IEC 60870-5-101 (serial) and the IEC 60870-5-104 (TCP/IP) protocol.

B- Junctions Workstations + Monitors and Accessories

Quantity: As Below

Workstations are used for SCADA Platforms to be installed and Engineered on it. The workstations receive data from server for Grid Monitoring and Control.

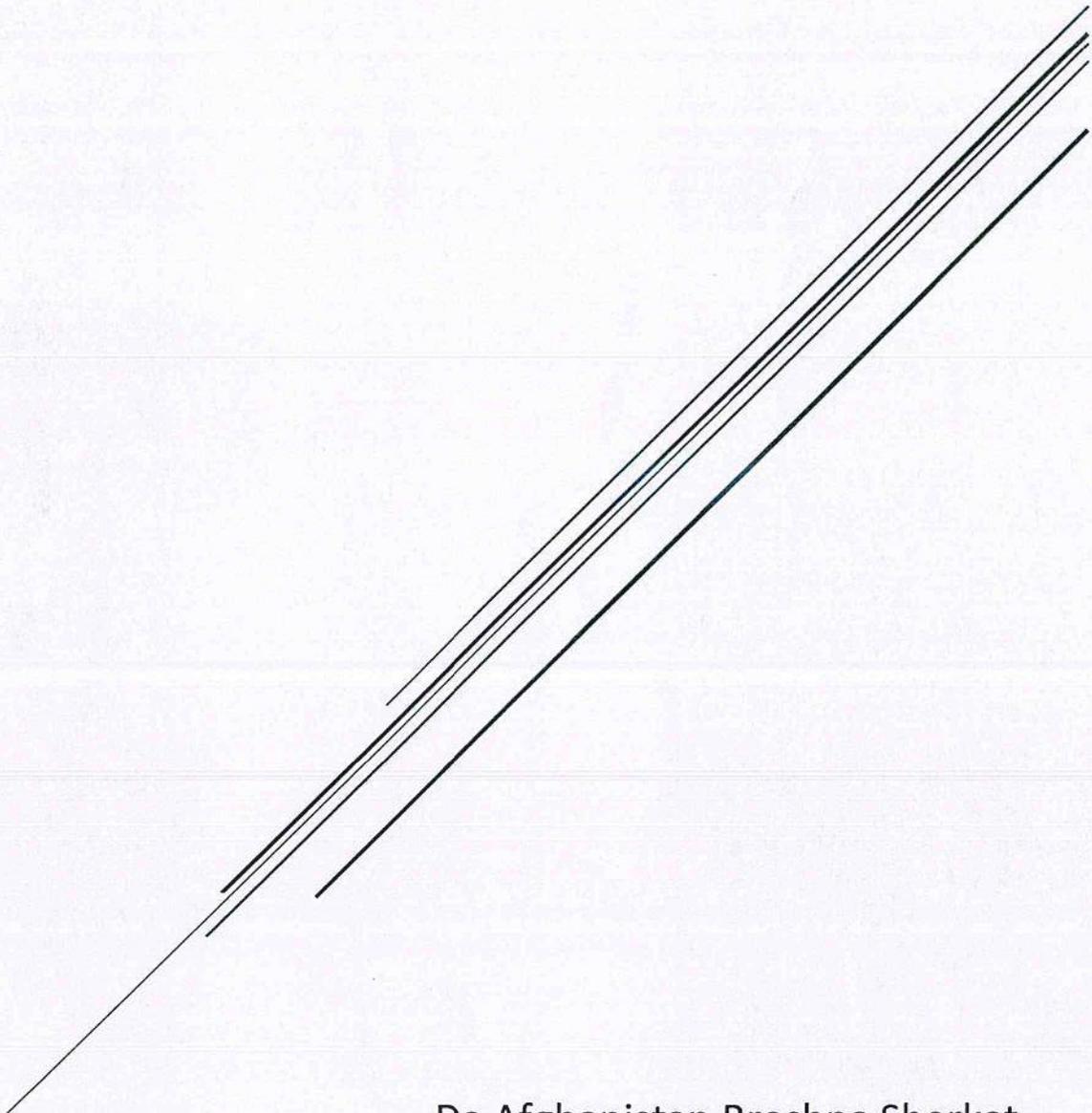
The devices shall full fill all requirement included in this document. It is to mention that Workstation is designed for special operation purpose. Contractor must only supply Workstation not desktop PC.

NUMBER	ITEM	SPECIFICATION	QUANTITY
1	Workstation	<ul style="list-style-type: none">- Workstation Tower,- Intel Xeon Silver4208 2.1GHz,- 16GB DDR4 RAM- 1TB 7200 SataHard Drive- 9.5 DVDWR 1st ODD,- Windows 10Pro,- Must Have at least 2x Ethernet ports- 2x HDMI Graphic ports- SD Card Reader,- Remote Graphics SW- mouse and keyboard,- + 2 years Extended Warranty,	10
2	Workstation Monitors	<ul style="list-style-type: none">- Diagonal Size 27" Resolution- Refresh Rate Full HD (1080p) 1920 x 1080 at 165 Hz- Adaptive Sync NVIDIA® G-SYNC® Compatible Certified- AMD FreeSync™ Premium Technology- Response Time 1 ms (gray-to-gray)- Ports 2 x HDMI, Headphones	20

Warranty: Workstations and Monitors shall have at least 2 years warranty.

SECTION 5

DC system



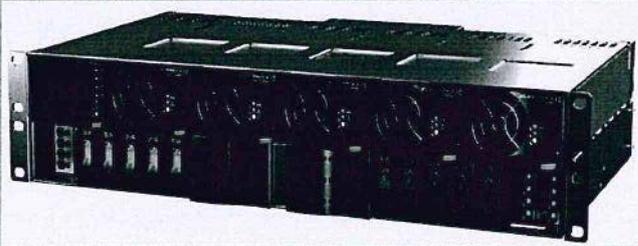
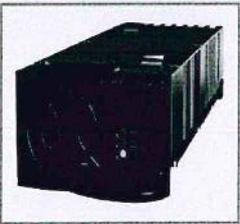
Da Afghanistan Breshna Sherkat
SCADA Department

5.1 48VDC Rectifier + Panel + Battery Bank

A- 48VDC Rectifier

Quantity: 1 Set/Lot (Total 12 Set)

Rectifier shall fulfill all requirement in this document. The dimensions and all specs are considered based on overall system designed.

MODEL	
shall be purely based on pluggable breakers and rectifiers	
INPUT DATA	
Voltage (range)	220Vac Nominal (At least 20%Fluctuation) (50 Hz)
Maximum current	21 ARMS
Mains configuration	Single phase
Connection	Rear connection on Faston connectors (6.3 mm)
OUTPUT DATA	
Nominal voltage	-48 V _{DC}
Maximum current	60 A _{DC}
BATTERY DISTRIBUTION	
LVBD	Default
Plug-in Breakers (max rating)	2x 60 A
Connection	Rear connection on M6 Studs, 25 mm ² max
LOAD DISTRIBUTION	
Plug-in Breakers Large (max rating)	2x 60 A
Connection Large Breakers	Rear connection on M6 Studs, 25 mm ² max
Plug-in Breakers Small (max rating)	10 x 30 A ¹⁾
Connection Small Plug-in Breakers	Front connection Push-in terminals, 6 mm ² max
CONTROL & MONITORING	
Smartpack S	Ethernet
OTHER SPECIFICATIONS	
Dimensions (W / H / D)	19" / 2U / 270 mm (incl. rear terminal cover) ³⁾
Mounting	19" Flush mount
  	

Handwritten signature

Handwritten signature

Handwritten signature

B- Panel

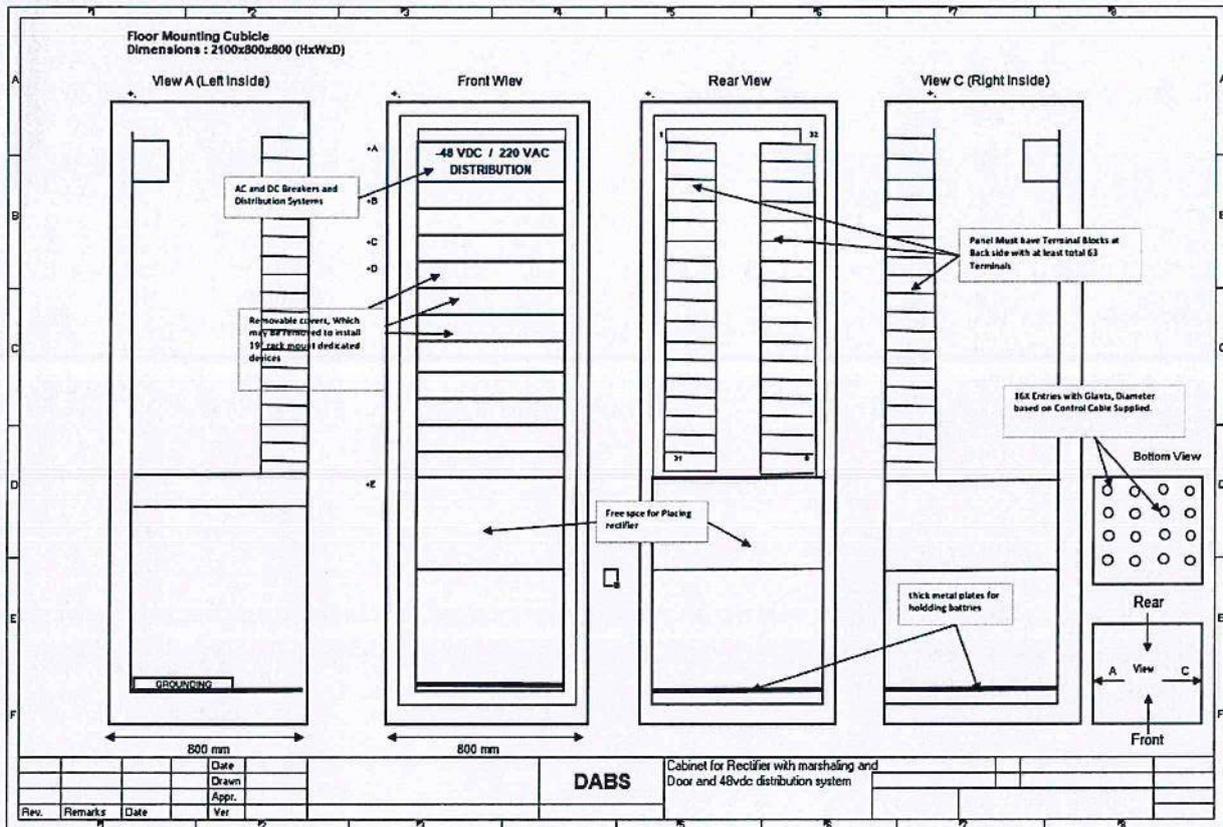
Quantity: 1 set/Lot (Total 12 Set)

Panel shall be designed based on the requirement for holding 19" rack mount Automation, Communication Devices, rectifier systems .etc.

Each panel must include all the items include in this document,

- At Front side DC and AC system and breakers must be included and pre-installed for both panels.
- At Rear side of Rectifier Panel Terminal Blocks for at least 63 terminals shall be included and pre installed.
- Front of panels shall have cover plates to prevent dust inside.
- The panel must be equipped with Lockable frond door and rear door.
- Panel shall be equipped with proper cooling fan to prevent devices overheating.
- At bottom of panels at least 16 entries with glands.
- Tick Metal palate for holding (4 x 12VDC 100AH batteries) shall be included and preinstalled at bottom of panel with space not disturbing cables entries from bottom.
- required cables for battery and rectifier connection to distribution part of panel

Drawing For Rectifier Panel:

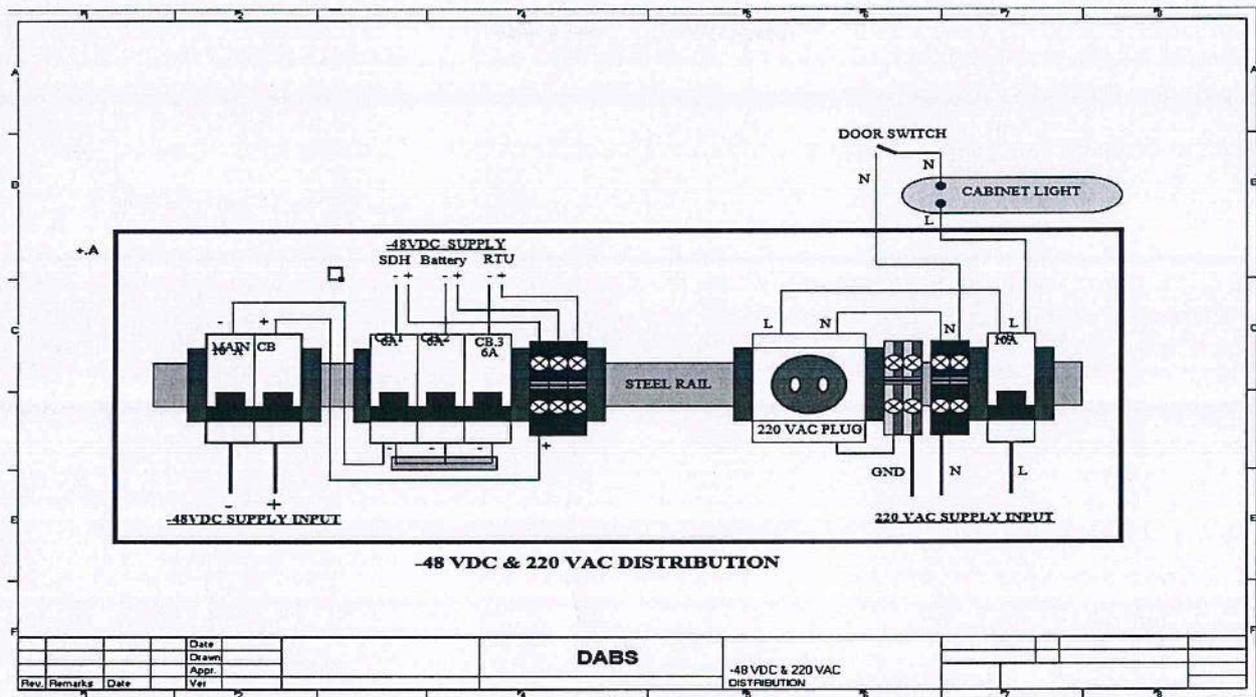


[Handwritten signature]

[Handwritten signature]

محمد سعید زیدی

Drawings AC and DC distribution System for each panel:



C- Battery Bank

Quantity: 4PCs/Lot (Total 48 PCs)

12VDC 100Ah VRLA AGM battery Each. battery will be installed in series to create 48VDC for each Junction Station DC system. with 6 meter 2.5mm² single core cable, lugs, nuts and bolts.



Warranty:

2 years for rectifier and batteries

[Handwritten signature]

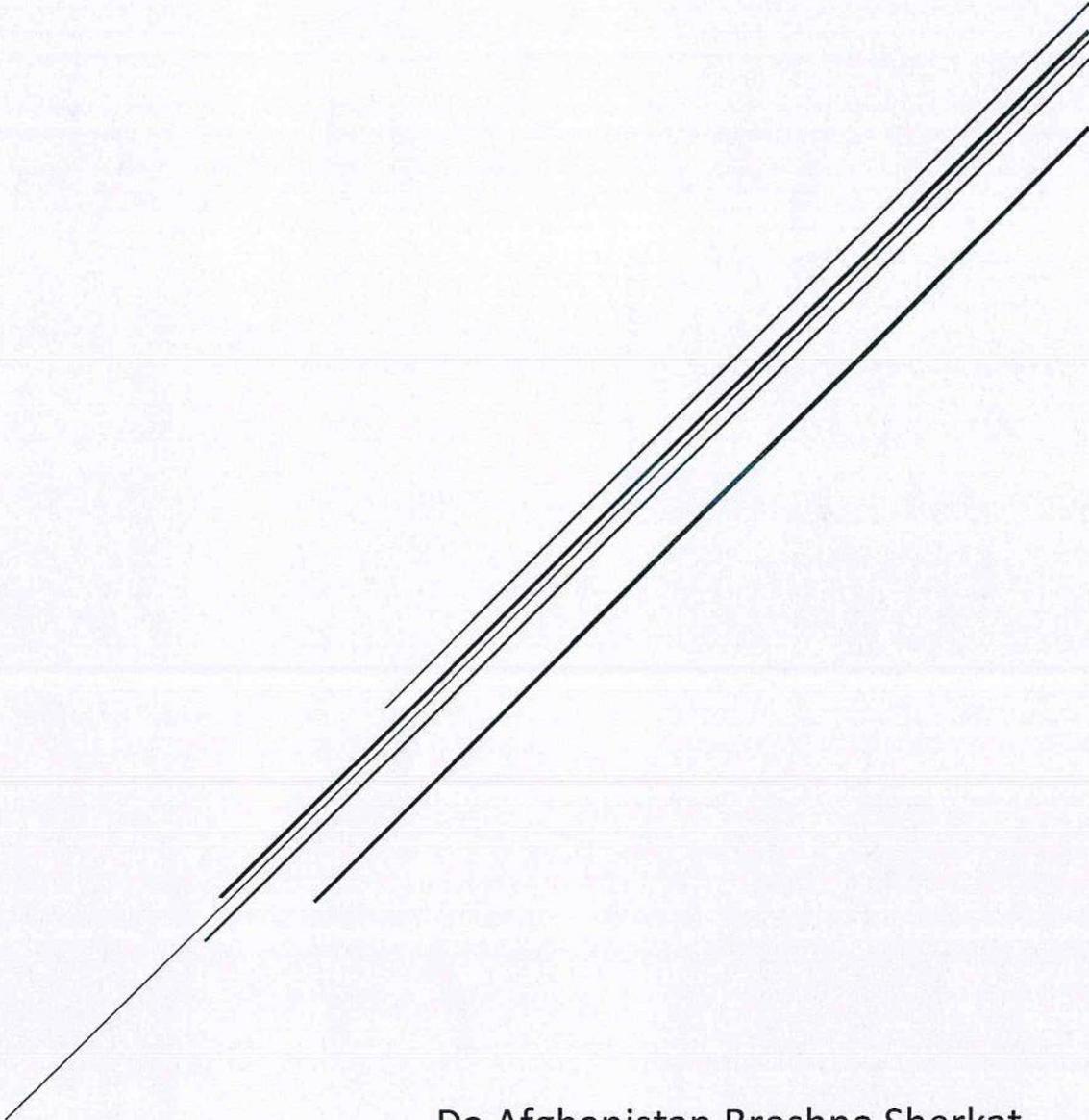
[Handwritten signature]

[Handwritten signature]

غلام حسین روزی

SECTION 6

Metering



Da Afghanistan Breshna Sherkat
SCADA Department

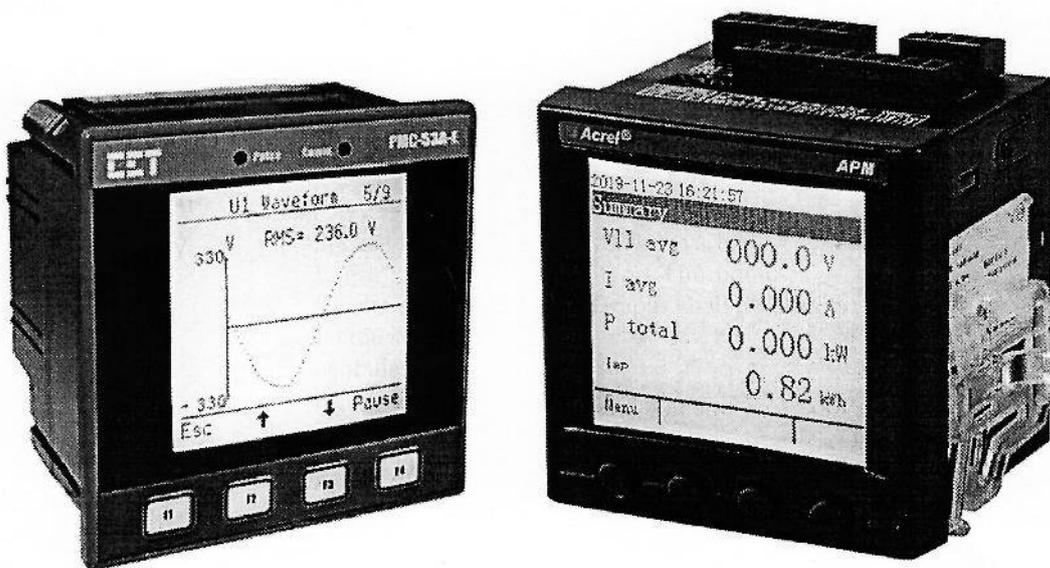
6.1 Analyzer

Quantity: Is included below table

The Power Quality Analyzer full fill all requirement and parts included in this document. Single Configuration software with license shall be supplied for whole batch.

NO	ITEM	PARAMETER	REQUIREMENT	QUANTITY
1	Analyzer 1A	Electrical network	Three-phase three-wire, three-phase four-wire	290 sets
		Frequency	45~55Hz	
		Voltage PT	Rated value : AC 100V	
		Current CT	Rated value: AC 1A,	
		Communication	RS485 interface/Modbus-RTU protocol RJ45 interface (Ethernet) / Modbus-TCP	
		Power supply	Working range: DC 48V DC or (100 to 300 VDC range adjustable or auto).	
		Voltage, current and power CLASS	class 0.2s	
		Active power CLASS	class 0.2s	
		Harmonic	1% (2rd~42nd) , 2% (43rd~63rd)	
		Storage	at least 4 GB	
		manuals	Engineering manuals to configure with SCADA	
		Power Cable	20 meter, 2.5mm ² double core cable	
		CT and PT Cable	30 meter 2.5mm ² Single Core cable	
		warranty	five year	
		Display	3phase I,KV,MW,Mvar,MWh,Mvarh,HZ,COSØ Energy Export, Energy Import, Harmonics, Events and Alarms and Graphs shall be display on the screen	
		TYPE	Mobular	
		Control Panel Accessories	Control Panel Mount nut and bolt and accessories	
Port	Both RS485 & Ethernet			
NO	Item	Parameter	Requirement	
2	Analyzer 5A	Electrical network	Three-phase three-wire, three-phase four-wire	15 sets
		Frequency	45~55Hz	
		Voltage PT	Rated value : AC 100V	
		Current CT	Rated value: AC 5A,	
		Communication	RS485 interface/Modbus-RTU protocol RJ45 interface (Ethernet) / Modbus-TCP	

Power supply	Working range: DC 48VDC , or (100 to 300 VDC range adjustable or auto).
Voltage, current and power CLASS	class 0.2s
Active power CLASS	class 0.2s
Harmonic	1% (2rd~42nd) , 2% (43rd~63rd)
Storage	at least 4 GB
Manuals	Engineering manuals To configure and interface with SCADA
Power Cable	20 meter, 2.5mm2 double core cable
CT and PT Cable	30 meter 2.5mm2 cable
warranty	five year
Display	3phase I,KV,MW,Mvar,MWh,Mvarh,HZ,COSØ Energy Export, Energy Import, Harmonics, Events and Alarms and Graphs shall be display on the screen
TYPE	Mobular
Control Panel Accessories	Control Panel Mount nut and bolt and accessories
port	RS485/Ethernet/ communication



Warranty

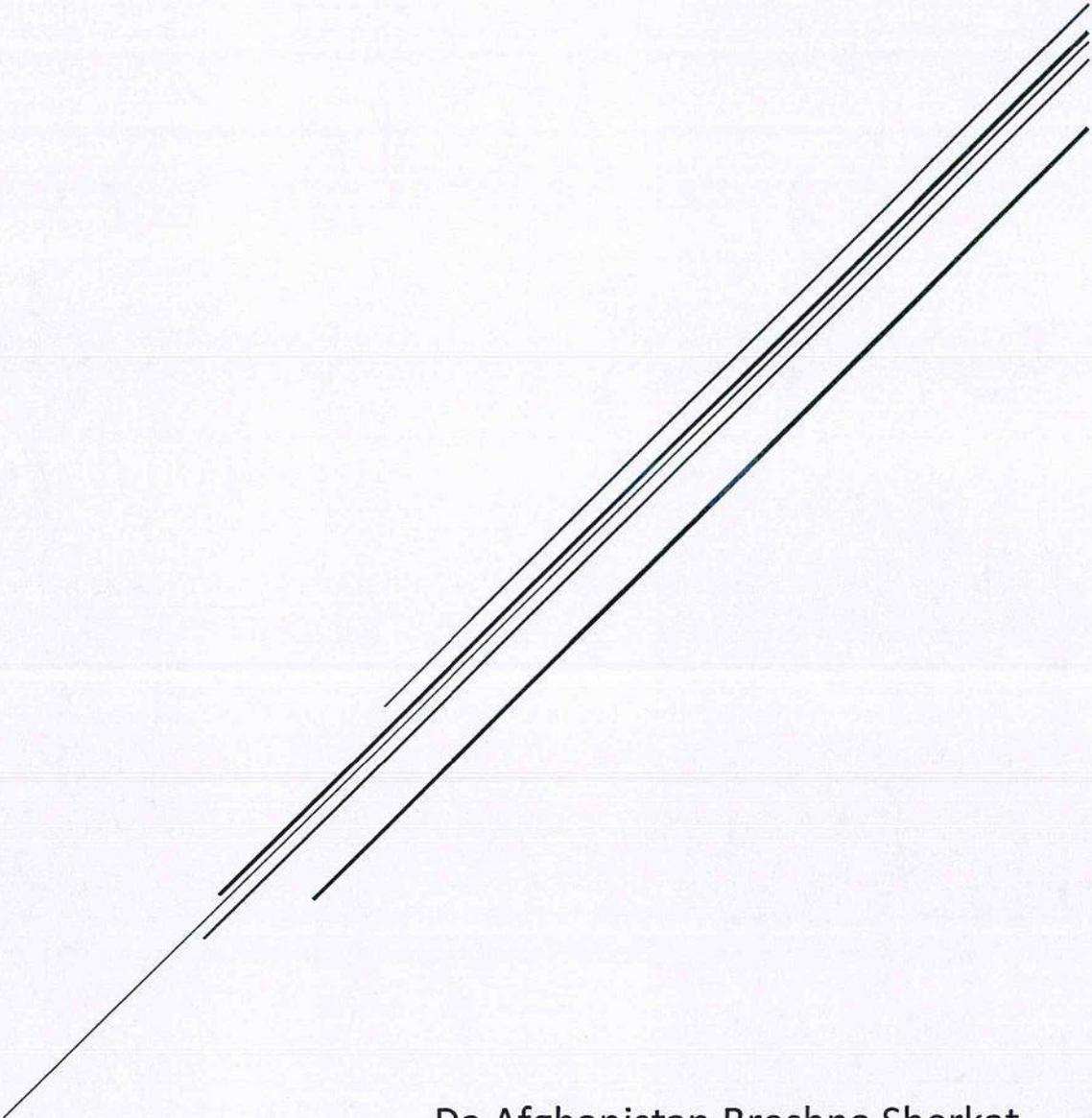
at least 2 years warranty.

[Handwritten signature]

[Handwritten signature]

SECTION 7

Telephone system



Da Afghanistan Breshna Sherkat
SCADA Department

7.1 Ip phone for Substaions

Quantity: 12PCS

IP phones are used to establish voice communication between Operators in the Grid. DABS SCADA system is equipped with Selta Office 8 PABX system so supplied IP phones shall be able to connect to Selta Office 8 PABX system for communication with NLCC and remote end substations.

NUMBER	REQUIREMENT	QUANTITY
1	<ul style="list-style-type: none"> - 128 × 64 pixel black and white backlit graphic display - 24 programmable keys with 3-color LEDs - 13 predefined function keys - Local directory and LDAP - Ready for external headphones and EHS function - Selta PABX ToIP - 2 ports 10/100 switch - Adapter and power cable - Wall mount and Desk peripherals 	12

**Warranty:**

Supplied IP phones shall have warranty for at least 2 years.

[Handwritten signature]

[Handwritten signature]

7.2 Ip phone for Junctions

Quantity: 12PCS

IP phones are used to establish voice communication between Operators in the Grid. DABS SCADA system is equipped with Selta Office 8 PABX system so supplied IP phones shall be able to connect to Selta Office 8 PABX system for communication with NLCC and remote end substations.

NUMBER	REQUIREMENT	QUANTITY
1	<ul style="list-style-type: none"> - 128 × 64 pixel black and white backlit graphic display - 24 programmable keys with 3-color LEDs - 13 predefined function keys - Local directory and LDAP - Ready for external headphones and EHS function - Selta PABX ToIP - 2 ports 10/100 switch - Adapter and power cable - Wall mount and Desk peripherals <div data-bbox="363 1120 1181 1657" style="text-align: center;"> </div>	12

Warranty:

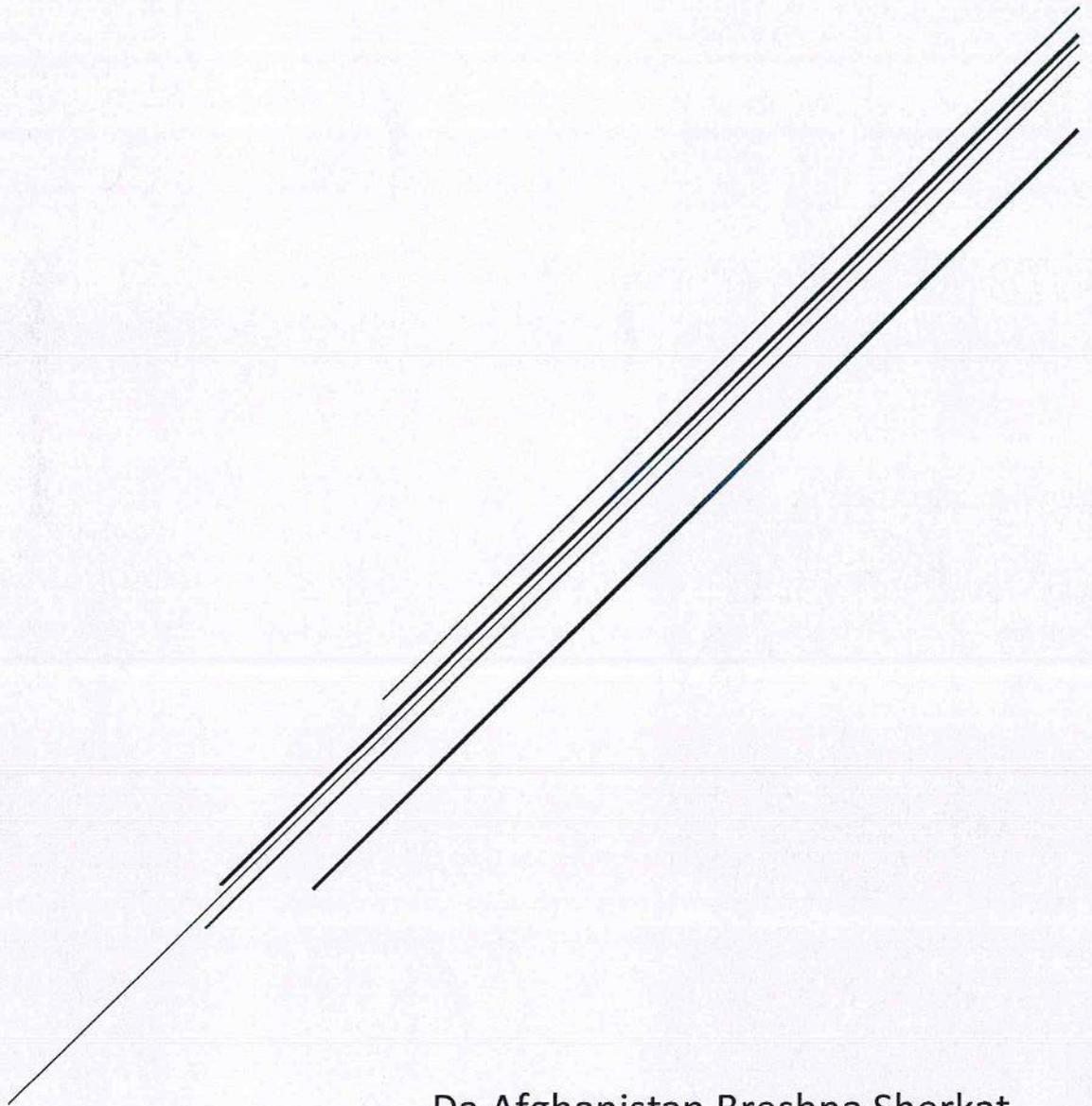
Supplied IP phones shall have warranty for at least 2 years.

[Handwritten signature]

[Handwritten signature]

SECTION 8

Accessories



Da Afghanistan Breshna Sherkat
SCADA Department

8.1 Lugs

Quantity: 2000 PCs

NUMBER	ITEM	PARAMETERS
1	Brand Name	
2	Finish/Color	Copper and PVC
3	Item Name	Boot Lace Pin
4	Box Quantity	2000 or in separate packs
5	Shape	Cylindrical
6	Length	14mm
7	Inside Diameter	4.6mm
8	Size	1.5mm ²
9	Connection Type	Crimp
10	Material	Copper and PVC
11	Finish	Copper and PVC
12	Colour	Black



Warranty: 1 Year

[Handwritten signature]

[Handwritten signature]

8.2 CAT6

Quantity: 3660m

NUMBER	ITEM	PARAMETER
1	Model Number	utp
2	Type	CAT 6
3	Place of Origin	Guangdong, China
4	Number of Conductors	8
5	Type	Cat6
6	Product name	Cat6 Network Cable
7	Color	Black/Custom
8	Application	Telecom Comunication
9	Certification	CE/ROHS/ISO9001/ISO/CE/CPR
10	Jacket	PVC LSZH LSOH PE HDPE
11	Conductor	cca/bc
12	Length	305m/carton
13	Insulation Material	HDPE
14	Conductor Type	Solid



Warranty: 1 Year

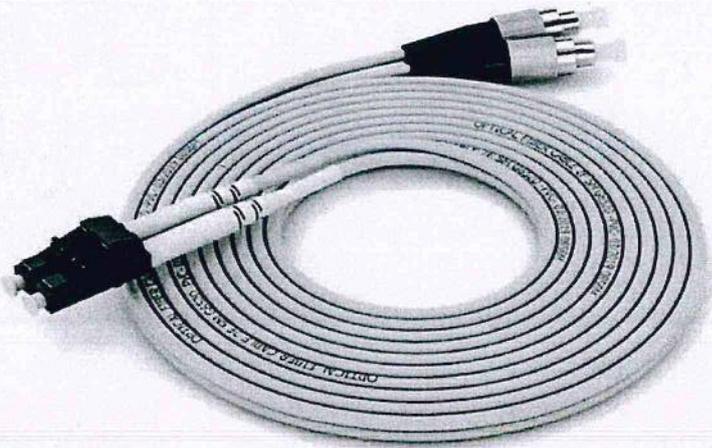
[Handwritten signature]

[Handwritten signature]

8.3 SM Patch Cord

Quantity: 36 PCs

NUMBER	ITEM	PARAMETER
1	Model Number	LC UPC to FC UPC Single mode Fiber Optic Patch Cord
2	Use	FTTX
3	Network	SDH
4	Product name	Fiber Optic Patch cord
5	Fiber Type	G652D
6	Connector Type	LC/UPC to FC/UPC
7	Color	Yellow
8	Material	PVC OFNR LSZH Plenum (OFNR)
9	Lenght	10meter each
10	Package	1pcs/bag
11	Fiber count	Duplex



Warranty: 1 Year

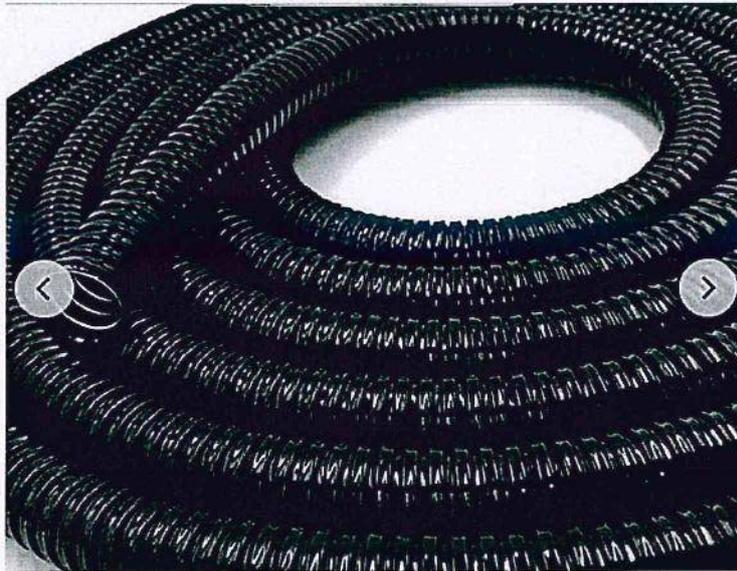
Handwritten signature in blue ink.

Handwritten signature in blue ink.

8.4 Protection Pipe

Quantity: 500 meter

NUMBER	ITEM	PARAMETERS
1	Type	Flexible
2	Material	Steel
3	Place of Origin	Hebei, China
4	Model Number	JWT-JS
5	Application	Electric Cable Wire Protection
6	Structure	Square lock
7	Surface	PVC Coated
8	Size	2 Inch diameter
9	Color	Black and Gray
10	Feature	Flame Resistant
11	Packing	PE wrap film



Warranty: 1 Year

8.5 Control cable

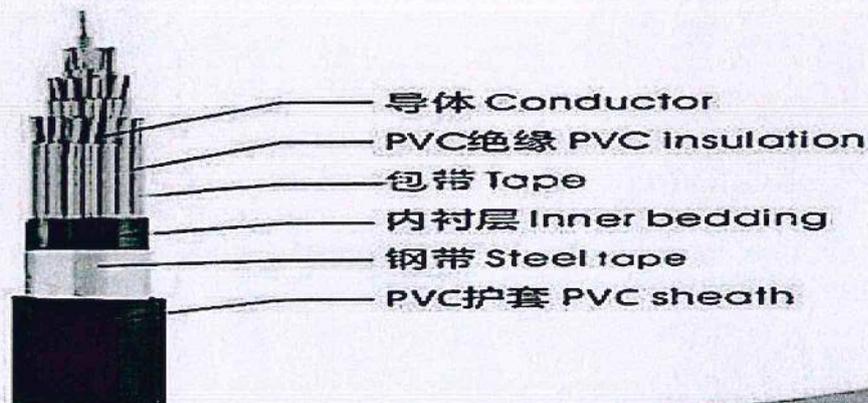
Quantity: 1200 meter

Control cables are multi-conductor cables used in automation and instrumentation applications. Control cables can measure and regulate transmissions of automated processes.

It connects the field signals to control room panels.

The control cable should be flexible in order to be bended easily in the panels and also should be resistant mechanically.

NUMBER	ITEM	QUANTITY	TECHNICAL DATA	
			Parameters	Requirements
1	Control Cable	1200 meter	Each CORE Diameter	1.5mm2
			Conductor	Copper
			Insulation	PVC
			Core Number	16 Cores
			Flexibility	Must be Flexible
			Shield	Standard Shield
			Overall Diameter	21.7mm
			Current Rating each core	16A
			Voltage Rating	600V
			Drum length	1200 meter per drum



Warranty: 1Year

Handwritten signature in blue ink

Handwritten signature in blue ink

Handwritten signature in blue ink

غلام حسین رومی

System Diagram. Rev4

