REQUEST FOR PROPOSALS

RFP DESCRIPTION:  Supervisory Control & Data Acquisition (SCADA) Specification Documentation

DUE DATE: NO LATER THAN SEPTEMBER 19, 2019 @ 10:00 A.M. EST
INVITATION TO SUBMIT
REQUEST FOR PROPOSAL FOR
Supervisory Control & Data Acquisition (SCADA)
Specification Documentation
RFP #2019-003

Dear Proposer:

The City of Thomasville is requesting the submittal of REQUEST FOR PROPOSAL (RFP) from qualified VENDORS interested in providing Supervisory Control & Data Acquisition (SCADA) Specification Documentation.

You are invited to submit a proposal. Please structure your proposal in accordance with the requirements and specifications outlined in this Request for Proposal. Any deviations, additions, or deletions should be so noted. Your proposal should address the issues and requirements in order as outlined on the following pages.

Specifications for the services requested are detailed below. The City reserves the right to reject any and all proposals, to waive minor irregularities, to consider minor variations of specifications that are clearly detailed, and to accept the most favorable proposal that appears to be in the best interest of the City of Thomasville. Proposals shall be sealed and plainly marked “RFP #2019-003 Supervisory Control & Data Acquisition (SCADA) Specification Documentation” and be received by the City Purchasing Office on or before the appointed time.

Please submit a written detailed proposal for SCADA Specification Documentation services and associated fees system. This RFP states the overall scope of services and vendor qualifications desired.

If you have any questions concerning this RFP, please email Anthony Choice, at anthonyc@thomasville.org.

Proposals shall be six (6) copies each of the Technical Proposal and Project Cost Proposal and submitted in a sealed envelope, addressed as follows:

City of Thomasville
Attn: Purchasing Administrator (Anthony Q. Choice) RFP #2019-003
P.O. Box 1540
Thomasville, GA 31799
PROPOSAL SUBMISSION REQUIREMENTS

General Instructions

Proposals should be prepared simply and economically and provide a straightforward, concise description of the Proposer’s company, qualifications, proposed solution, and capabilities to satisfy the requirements of this RFP. Emphasis should be on completeness and clarity of content. The City discourages lengthy and costly submissions – glossy sales and marketing brochures are not necessary or desired.

Information must be organized consistent with the outline provided in the next section (4.2 Proposal Format and Content). Proposers must follow all formats and address all portions of the RFP set forth in this document and provide all requested information. Proposers may retype or duplicate any portion of the RFP for use in responding to the RFP, provided that the proposal clearly addresses all of the City’s information requirements.

Under separate cover, please prepare and submit a separate sealed Project Cost Proposal. RFPs and Project Cost Proposals must be delivered by the date/time specified and to the place stipulated on the cover of this RFP. It is the sole responsibility of the vendor to see that their RFP is received in the proper time. Any proposal received after the proposal opening date and time shall be eliminated from consideration and returned to the vendor unopened.

1.2 Proposal Format and Content

Proposals must be structured, presented, and labeled in the following manner:

- Cover Letter
- Table of Contents
- Section 1 – Executive Summary
- Section 2 – Company Background
- Section 3 – Company Qualifications
- Section 4 – References
- Section 5 – Configuration Approach and Work Plan
- Section 6 – Ongoing and Post-Implementation Support
- Section 7 – Cost

Proposals should be prepared on standard 8½” x 11” paper and printed on two sides. All proposal pages should be numbered.

Cover Letter

The proposal must include a cover letter that provides the following:

- a. Proposer’s legal name and corporate structure.
- b. Proposer’s primary contact to include name, address, phone, and email.
- c. Other Companies, Corporations, Partnerships, or Joint Ventures with which the Proposer is affiliated.
d. Identification of use of any subcontractors and scope of work to be performed by subcontractors.
e. Identification of any pending litigation again the Proposer or Proposer’s affiliates.
f. Disclosure of any bankruptcy or insolvency proceedings in last ten (10) years for the Proposer or the proposer's affiliates.
g. Statement of the Proposer’s credential to deliver the services stated under the RFP.
h. Statement indicating the proposal remains valid for at least 120 days.
i. Statement that the Proposer or any individual who will perform work for the Proposer is free of any conflict of interest (e.g., employment by the City).
j. Signature of a company officer empowered to bind the Proposer to the provisions of this RFP and contract awarded pursuant to it.

The Proposal Cover Letter should be concise and brief and not exceed two (2) pages.

**Table of Contents:** All pages are to be numbered. Figures, tables, charts, etc. must be assigned index numbers and identified in the Table of Contents.

**Section 1 – Executive Summary:** Provide a concise overview of the proposed professional services and associated costs. The Executive summary should not exceed two (2) pages.

**Section 2 – Company Background:** This section of the proposal should:

2.1 – Provide a brief description of the Proposer’s background.
2.2 – Identify the location of headquarters, technical support, and field offices and the location of office which would service the City.
2.3 – Identify Proposer’s annual company revenues and profit for the last three (3) company fiscal years.
2.4 – Describe relationship with any third party vendor(s) or application(s) provider, specifically third party partnership with proposing company.

The Background section should not exceed three (3) pages.

**Section 3 – Company Qualifications:** In this section of the proposal, the Proposer should identify company qualifications and experience in configuring SCADA similar to what the City is seeking:

3.1 – Describe the Proposer’s familiarity with SCADA implementations/configurations including how many your organization has completed.
3.2 – Describe the Proposer’s familiarity with GIS configuration pertaining to utilities including how many our organization has completed.
3.3 – Identify experience with similarly-sized cities.

The Qualifications section should not exceed four (4) pages.

**Section 4 – References:** The Proposer must provide at least five (5) references with three (3) of the references for SCADA system implementations and with two (2) of the references for GIS configuration. All references must be from implementation or configuration within the last five (5) years and be in live-production use of the configuration the City needs. The City prefers references from agencies of similar size and complexity to the City. For each reference, proposer must provide the following information:

4.1 – Name and contact information (i.e. name, title, address, phone, and email).
4.2 – Brief project description, including identifying the software version and what was configured.
4.3 – Number of employees.
4.4 – Configuration date.
4.5 – Configuration timeline and cost.

The References section should not exceed two (2) pages.

**Section 5 – Configuration Approach and Work Plan:** The Proposer should identify the proposed implementation approach clearly so that the City’s objectives and goals are met. Screen shots or images that reflect past projects are encouraged.

5.1 – Provide resumes for the project manager and other key resources assigned to this project.
5.2 – Describe your project approach, methodology, and work plan based on your experience with similar configurations and sized agencies.
5.3 – Identify the roles/responsibilities of and resources required by City staff.
5.4 – Describe your recommended training approach and how to ensure users (from general user to advanced user to administrator) are prepared to use the SCADA solution.

While there is not page limit for the Configuration Approach and Work Plan section, this section should still be straightforward and concise per the General Instructions – Section 4.1.

**Section 6 – Ongoing and Post-Implementation Support:** In this section, the Proposer should address post-implementation support services and should not exceed two (2) pages.

**Section 7 – Cost** (attach as a separate document)

The City seeks a clear and comprehensive understanding of all costs associated with the configuration of SCADA and applicable systems. In this section, the Proposer must itemize all costs associated with the implementation. Specifically, the City wants to understand the level of effort, identification of the resources to be provided by proposed phase, and the related resource rates. The Proposer's Price Sheet(s) must identify all costs required to complete a successful implementation.
PROPOSAL EVALUATION AND SELECTION PROCESS

An Evaluation Committee will review all submissions to determine which Proposers have qualified for consideration. The proposals will be publicly opened and vendor announced in the Purchasing Department at the appointed time. The proposals will be considered by the City Council at a regularly scheduled City Council meeting within 45-60 days of the proposals’ opening.

The primary criteria for vendor evaluation, consideration and scoring weights are:

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>WEIGHT</th>
<th>POINT VALUE/RATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Stability</td>
<td>10%</td>
<td>0-3</td>
</tr>
<tr>
<td>Ability to Provide Solution to meet stated requirements</td>
<td>30%</td>
<td>0-3</td>
</tr>
<tr>
<td>Experience with Similar Projects</td>
<td>20%</td>
<td>0-3</td>
</tr>
<tr>
<td>Demonstrated Success and Experience of Project Team in Other Communities and/or with Similar Projects</td>
<td>20%</td>
<td>0-3</td>
</tr>
<tr>
<td>Cost – in include support fees</td>
<td>20%</td>
<td>0-3</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100 percent</strong></td>
<td><strong>15 points</strong></td>
</tr>
</tbody>
</table>

Proposers should be aware that finalists may be required to participate in on-site interviews to allow staff to fully understand and validate the proposed implementation approach and meet key proposed personnel. At the completion of the interviews, the City may have additional questions for the finalists to ensure that all pertinent information is reviewed prior to finalizing negotiations.

The City of Thomasville will receive competitive proposals from firms having specific experience and qualifications in the areas identified in this solicitation. Under competitive negotiation procedures, the terms of the service contract, the price of the services, the method of service delivery, and the conditions of performance are all negotiable. A negotiated contract will be awarded to the agency that best meets the proposed needs at a reasonable price, not necessarily at the lowest price.

For consideration, proposals must contain descriptions of the agency’s experience and abilities to perform pursuant to the City of Thomasville requirements. Unless otherwise stated, all proposals shall address each criterion identified in this RFP.
OTHER PROPOSAL INFORMATION

RFP Terms and Conditions

Acknowledgement of Amendments: Each agency receiving a copy of this shall acknowledge receipt of any amendment to this RFP by signing and returning the amendment with the completed proposal. The acknowledgement must be received by the City of Thomasville at the time and place specified for receipt of proposals.

Additional Information: Questions regarding this solicitation shall be submitted in writing to anthonyc@thomasville.org: Respondents are cautioned that any oral statements made that materially change any portion of this solicitation are not valid unless subsequently ratified by a formal written amendment to this RFP. No technical questions that may materially change any portion of this solicitation will be accepted during the fourteen calendar days prior to the time and date set for receipt of proposals.

Applicable Laws: Shall Apply: The contract awarded shall be governed in all respect by the laws of the State of Georgia, and any litigation with respect thereto shall be brought in the courts of the State of Georgia, Thomas County Superior Court. The company awarded the contract shall comply with applicable Federal, State, and local laws and regulations.

Change in Objectives: The City of Thomasville may materially change the Objectives. Such changes may include additions, deletions, or other revisions within the general scope of RFP requirements. No changes or adjustments shall be made without a written amendment to this RFP, signed by the Purchasing Administrator.

Collusion among Respondents: Each respondent, by submitting a proposal, certifies that it is not party to any collusive action or any action that may be in violation of State and Federal law.

Exceptions: A respondent taking exception to any part or section of this solicitation shall indicate such expectations in a separate section of the submitted proposal – such section shall be entitled “Exception of Conditions.” Failure to indicate any exception will be interpreted as the respondent’s intent to comply fully with the requirements of this RFP as written.

Expenses Incurred: There is no expressed or implied obligation for the City to reimburse responding firms for any expenses incurred in preparing proposals in response to this request. Materials submitted by respondents are subject to public inspection under the Georgia Public Records Act (Government Code Sec. 6250 et seq.), unless exempt. Any language purporting to render the entire proposal confidential or proprietary will be ineffective and will be disregarded.
Late Submissions: Any proposal received at the place designated in this RFP after the time specified for receipt will not be accepted or considered.

Nonconforming Terms and Conditions: Any proposal that includes terms and conditions that do not conform to the terms and conditions in this RFP is subject to rejection as non-responsive. The City of Thomasville reserves the right to permit the respondent to withdraw non-conforming terms and conditions from its proposal prior to action by the City Council to award a contract.

Withdrawal of Proposal: Respondents may withdraw all or any portion of a proposal at any time during and after the review and award process, up to ratification of an agreement between the City of Thomasville and the designated agency.

Withdrawal of Request for Proposal: The City of Thomasville retains at all times the right to cancel or withdraw this RFP, to refuse to accept a proposal from any respondent, and to modify or amend any portion of this RFP.

The City reserves the right to retain all proposals submitted and to use any ideas in any proposals submitted, regardless of whether or not that proposal is accepted. Submission of a proposal indicates acceptance by the person submitting the proposal of the terms, conditions and specifications contained in this RFP, unless clearly and specifically noted in the proposal submitted and confirmed in a subsequent contract between the City and the contractor selected.

Evidence of Ability to Perform
Before the award of any contract, each respondent may be required to demonstrate to their services to the designated committee, that it has the necessary experience, ability, and resources to provide the services specified herein within the timeline required. This may include site visits. The City of Thomasville may make reasonable requests deemed necessary and proper to determine the scope-of-work, and the respondent shall furnish to the City of Thomasville all information for this purpose.

Final Selection
Following the review of the proposals, presentation and interviews, the City may further invite a firm(s) to formally meet with City representatives/project team at firm’s own expense prior to making a final determination to address additional inquiries by the City and to discuss and/or negotiate terms and conditions for a final contract. Factors that will determine the final selection will include the finalization of terms in regard to service agreements and costs. However, the City reserves the right to reject any or all quotations, waive any informality in RFP's, and to accept or reject any items thereon.
Contract Commencement and Completion

The selected firm will be required to enter into a Sales Agreement for this project with the City of Thomasville.

Any contract resulting from this RFP shall not be effective unless, and until, approved by the City Council or its designee. Upon approval, contract services shall commence within 30 days after the award of the contract. The estimated completion date shall be defined in the proposal submitted by the selected firm.

Before the City executes a contract, the selected firm shall furnish the City a certificate evidencing Workmen’s Compensation Insurance with limits no less than $1,000,000 per accident or disease and Comprehensive Public Liability Insurance or General Liability Insurance with limits no less than $1,000,000 per occurrence. The City shall be named as additional insured with the following information listed on the Accord Certificates of Insurance must be accompanied by the applicable endorsements for the specific insurance policy.

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Telephone</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Company</th>
<th>Address</th>
</tr>
</thead>
</table>
SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

1.1 Overview

The following section describes the SCADA component of an ADMS.

1.2 System Architecture

Provide a high-level architecture diagram of the SCADA. Using a diagram, describe how:

- The SCADA system can be integrated to other modules such as outage management system (OMS) and the distribution management system (DMS).
- Redundancy can be achieved. Describe the type of redundancy that could be implemented. Implementing up to quad-redundancy.
- The SCADA system will interface with field devices by means of industry standard communication protocols. Describe the type of interfaces and protocols required.
- The SCADA system can be both, a client or a server to other systems using data exchange protocols, files or interfaces.

1.3 SCADA System Functional Requirements

1.3.1 Replacing an incumbent SCADA or implementing a new SCADA

1.3.1.1 When replacing an existing SCADA system, the vendor shall minimize the disruption to the existing operational ecosystem.

Provide a description of the actual setup, and include the following: existing vendor name, number of displays, protocols in use, communication mediums, type of RTU or data concentrators, approximate number of points, and any interoperability with other utility systems.

1.3.2 Master Station

1.3.2.1 The master station consists of a host computer (server). Hot-Standby failover redundancy can be achieved by up to four servers: Single host (server), Redundant configuration with two host computers (servers), or a dual redundant...
configuration with Quad host computers (servers). When Hot-Standby redundancy is used in dual or quad host (servers), 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.

1.3.2.2 Separate Operator workstations (clients) can 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.

1.3.2.3 When legacy devices not supporting TCP-IP network are present on the system, Media converters or terminal servers shall be used to convert Ethernet TCP-IP networks to serial interfaces such as RS-232, 422, 485, Monomodal fiber or radio systems. Terminal servers shall be able to interface to the Gigabit network.

1.3.2.4 Master Station host server(s) can be implemented in virtual environments following the vendor’s network and hardware requirements of the servers 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 shall provide the hardware specifications for a virtualized primary server and for a virtualized secondary server located at a separate facility.

1.3.3 Configuration

1.3.3.1 The host server(s) and all workstations shall consist of standard PC architecture machines utilizing the latest generation Intel or equivalent processors.

1.3.3.2 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.

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

1.3.4 Communications

1.3.4.1 The system shall support the DNP3.0 (serial and TP/IP) protocol and all other industry standard non-proprietary protocols.

1.3.4.2 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 shall be available for Data Exchange tasks.

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

1.3.4.4 The master station database editor should 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, and protocol-specific configuration parameters. The communication software should maintain communication statistics for each RTU. These statistics should be available as database points so that they can be incorporated in user-defined displays, reports, and alarms.

1.3.5 Security

1.3.5.1 The SCADA system should 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.

1.3.5.2 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.

1.3.5.3 The vendor should provide cybersecurity features, including but not limited to, authentication, encryption, access control, event and communication logging, monitoring and alarming to protect the system and configuration computer from unauthorized modification or use.

1.3.5.4 The vendor should 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 should 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.

1.3.5.5 The vendor should 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).

1.3.5.6 The vendor should 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.

1.3.5.7 The vendor should provide a listing of services required for any computer system running control system applications or required to interface the control system applications. The listing should include all ports and services required for normal operation as well as any other ports and services required for emergency operation.

1.3.5.8 The vendor should verify and provide documentation that all services are patched to current status. The vendor should 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.

1.3.5.9 The vendor should 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 should 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 (e.g. MSN, AOL 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.

1.3.5.10 The vendor should configure hosts with least privilege file and account access and provide documentation of the configuration. The vendor should 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 should document that the changing or disabling of access to such files and functions has been completed.

1.3.5.11 The vendor should 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).

1.3.5.12 The vendor should provide details of their patch management and update process. Responsibility for installation and update of patches should be identified.

1.3.5.13 The vendor should 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 should provide firewall rule sets and/or other equivalent documentation. The basis of the rule set should be “deny all,” with exceptions.
explicitly identified by the vendor. Note that this information is deemed business sensitive and should be protected as such.

1.3.5.14 The vendor should 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.

1.3.5.15 The vendor should recommend which accounts need to be active as well as those which can be disabled, removed or modified. The end user should approve in writing the vendor’s recommendation. The vendor should disable, remove, or modify all the accounts pursuant to the approved recommendation.

1.3.5.16 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.

1.3.5.17 After the site acceptance testing (SAT), the vendor should disable, remove or modify all vendor-owned accounts or negotiate account ownership with the end user.

1.3.5.18 The vendor should not permit user credentials to be transmitted in clear text. The vendor should provide the strongest encryption method to commensurate with the technology platform and response time constraints. The vendor should not allow applications to retain login information between sessions, provide any auto-fill functionality during login or allow anonymous logins. The vendor should provide user account-based logout and timeout settings.

1.3.5.19 The vendor should 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.

1.3.5.20 The vendor should not store passwords electronically or in vendor-supplied hardcopy documentation in clear text unless the media is physically protected. The vendor should control configuration interface access to the account management system. The vendor should 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.

1.3.5.21 The vendor should provide a system whereby account activity is logged and is auditable both from a management (policy) and operational (account use activity) perspective. The vendor should time stamp and control access to audit trails and log files. The vendor should ensure audit logging does not adversely impact system performance requirements.

1.3.5.22 The vendor should provide for user accounts with configurable access and permissions associated with the defined user role. The vendor should adhere to least privileged permission schemes for all user accounts and application-to-application communications.
1.3.5.23 The vendor should verify that a user cannot escalate privileges, under any circumstances, without logging into a higher-privileged role first. The vendor should provide a mechanism for changing user(s) role (e.g. group) associations. After contract award, the vendor should provide documentation defining access and security permissions, user accounts, applications and communication paths with associated roles.

1.3.5.24 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 should describe the use of any web-based interfaces for critical control functions. If they are used, vendors should respond to the requirements listed below.

1.3.5.25 The vendor should 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.

1.3.5.26 The vendor should 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 should provide documentation on what is removed and/or disabled.

1.3.5.27 The vendor should 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.

1.3.6 System Sizing

1.3.6.1 The system software shall be capable of accommodating in its database an unlimited quantity of status and control points, analog input points, text points, communication lines, RTUs, IEDs, reports, graphic symbols. No software upgrades or additional licenses shall be required to increase the number of aforementioned items to be integrated into the system.

1.3.6.2 Vendor shall provide documentation of 99.98% system availability

1.3.7 Hardware Platform

1.3.7.1 The hardware platform encompasses all of 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.

1.3.7.2 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.

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

1.3.8.1 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.

1.3.8.2 The City prefers that host servers run the latest Microsoft Windows Server 64-bit operating system (OS), but other OS such as UNIX, Linux, OS2, and VMS will be considered.

1.3.8.3 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.

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

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

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

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

1.3.9 Workstation Consoles

1.3.9.1 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.

1.3.9.2 The workstations shall run the latest version Microsoft Windows 64-bit operating system.

1.3.9.3 The workstation consoles shall utilize Gigabit Ethernet network interface cards (NIC).

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

1.4 SCADA System Functional Requirements

1.4.1 Data Acquisition

1.4.1.1 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.
1.4.1.2 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.

1.4.1.3 The data acquisition module should not require any protocol converter or front-end processors for industry standard non-proprietary protocols. These should be native to the system. If the vendors system requires a front-end processor for these types of protocols, the vendor should explain why this extra point of failure is necessary and what the benefits to having this are.

1.4.1.4 The SCADA system should 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.

1.4.1.5 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.

1.4.2 Supervisory Control

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

1.4.2.2 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

1.4.2.3 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.

1.4.2.4 Based on noisy serial or radio communications, the system provides settings to configure the response time before a control failure alarms are raised.
1.4.2.5 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.

1.4.3 Communications

1.4.3.1 The software subsystem for the proposed protocols shall implement all features of the RTUs and IEDs that are required by the end user. 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

1.4.3.2 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.

1.4.3.3 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.

1.4.3.4 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.

### 1.4.4 Data Processing

1.4.4.1 The system provides 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 as a result 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.

1.4.4.2 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).

1.4.4.3 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 deadband.

1.4.4.4 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 deadband is 3.0, any input value which is converted to between +3.0 and -3.0 engineering units will be clamped to zero.

1.4.4.5 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.

1.4.4.6 The system should 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.

1.4.4.7 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.

### 1.4.5 Authentication and Access Control

1.4.5.1 The system will use username and password to be authenticated over LDAP (Active Directory) and Two factor Authentication.
1.4.5.2 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.

1.4.5.3 The Guest account by default restrict certain areas of the map or alarms, this account should be configurable to allow further restrictions.

1.4.5.4 The system can temporarily disable a user account without deleting it.

1.4.5.5 The system can deny remote access for a user account.

1.4.5.6 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.

1.4.5.7 The number of upper, lower case, and special characters is configurable to enforce security. System shall prevent reuse of passwords, the inclusion of the user name on the password field and, repeated strings of identical characters.

1.4.5.8 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.

1.4.5.9 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.

1.4.5.10 Account activity logging are be configurable for login success and failures. The logging mechanisms shall be configurable for the remote Syslog protocol.

1.4.5.11 The system generates and print a report of the log list that can contain information on the application used and the time accessed.

1.4.5.12 A method for editing network security, which defines the rules for the SCADA system to characterize TCP/IP connections.

1.4.5.13 TCP connections can be classified as Remote, Local or Reject.

1.4.5.14 The login supports network encryption RC4 as minimum requirement.

1.4.5.15 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.

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.
1.4.6 User Rights

1.4.6.1 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.

1.4.6.2 The proposed system can handle an unlimited number of user accounts with their corresponding user rights and privileges.

1.4.7 Area of Responsibility

1.4.7.1 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 zones to each database point (telemetered or calculated) and/or to each login account.

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

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

1.4.8 Tag Management

1.4.8.1 The system can 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.

1.4.8.2 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.

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

1.4.8.4 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).

1.4.8.5 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.

1.4.8.6 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.

1.4.9 Database Editor
1.4.9.1 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.).

1.4.9.2 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.

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

- The ability to clone features to create an entirely new features and all its points, based on an existing feature.
- 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 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

1.4.9.4 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.

1.4.10 Alarms

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

1.4.10.2 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.

1.4.10.3 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.

1.4.10.4 Each priority has its own setup and properties: variables such as how they are raised and represented can be custom programmed to each independently.
1.4.10.5 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.

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

1.4.10.7 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.

1.4.10.8 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.

1.4.10.9 The system provides a summary lists 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.

1.4.11 Reports

1.4.11.1 The system includes 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 pre-determined file locations.

1.4.11.2 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.

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

1.4.11.4 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.

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

1.4.12 Data Collection and Storage

1.4.12.1 The system will 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.
1.4.12.2 The historical data software shall be capable of sampling at intervals as low as 1 second. There should be no upper bound on the duration of samples within each dataset, and thus no upper bound on the amount of historical data that can be stored other than the limitation imposed by available disk space.

1.4.12.3 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.

1.4.12.4 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.

1.4.13 Data Trending

1.4.13.1 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.

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

1.4.13.3 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.

1.4.13.4 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 time-stamp of the traces at any time position in the graph by manipulating a time cursor inside the trend graph.

1.4.13.5 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.
1.5 Graphical User Interface (GUI) Functional Requirements

1.5.1 GUI

1.5.1.1 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.

1.5.1.2 GUI shall support running OS environment of Windows 10 or higher and should offer a tabbed interface, allowing quick access to multiple views (map, alarms, operations logs, and graphs) within a single screen.

1.5.1.3 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 of 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
- Provide a tabular view on trend graphics.
- Editing capabilities - create/modify/delete objects on a map
- Built-in interactive help videos
- 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.
1.5.2 Drawing Tools

The system shall provide the capability to:

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

<table>
<thead>
<tr>
<th>Fonts</th>
<th>Symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symbol Tables</td>
<td>Colors</td>
</tr>
<tr>
<td>Color Tables</td>
<td>Widgets</td>
</tr>
<tr>
<td>Control Panels</td>
<td>Templates</td>
</tr>
</tbody>
</table>

1.5.2.2 Group Views and Layers in a tree hierarchy.

1.5.2.3 Declutter the map using layers.

1.5.2.4 Define the topology of a network using line sections.

1.5.2.5 Support multi-user editing and job partial or total reservation with a log of changes and users.

1.5.3 Notes

1.5.3.1 The system shall provide the capability to view, create, and maintain Notes in the system.

1.5.4 Operator Display

1.5.4.1 GUI shall be capable of displaying a geographic map that shows all the distribution circuits.

1.5.4.2 GUI shall have the capability to open a separate magnification window to display details while the main view remains open.

1.5.4.3 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.

1.5.4.4 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).

1.5.4.5 The map view should be able to be configured to automatically declutter detail when zooming in and out (i.e., text annotation, secondary roads, etc.).
1.6 SCADA Systems Applications

This section outlines and describes certain SCADA functions and applications that are of interest to the City of Thomasville. For each application, let the City know if your SCADA system is capable of doing this or not. Is this an add-on module or is it included in the base platform? We have described some of the functionality of each application and, in some cases, given a high-level view of some of the processes. If your SCADA’s implementation of these applications is different, describe the differences.

1.6.1 Command Script Execution

1.6.1.1 Command Script Execution is an easy-to-use high-level programming language. It should allow the user to define and execute programs which use database points as variables. Command Script Execution programs can be used for calculations, open-loop control or switching sequences and for closed-loop control.

1.6.1.2 The Command Script Execution program should be started and stopped from an editing program, or via a pushbutton menu in GUI map, or it may be triggered automatically by a status change.

1.6.1.3 The Command Script Execution program should 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 Command Script Executions as subroutines
- Two-dimensional table lookup with planar interpolation
- CPU utilization calculations per host.
1.6.2 IED Control Panel Templates

1.6.2.1 The system should support IED 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 should support multiple pages of IED information.

1.6.2.2 The user should 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.

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

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

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

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

1.6.2.7 The vendor should 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.

1.6.3 Power Quality Event Capture

1.6.3.1 Power Quality Event Capture should allow the user to analyze the entire state of the system leading up to, and after an event. All changes in analog and status points system-wide are recorded when a user-defined event is detected.

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

1.6.3.3 Status can trigger an event capture for a change of state.

1.6.3.4 Analog points can trigger an event capture for any limit violation.

1.6.3.5 Power Quality Event Capture should keep a log of all events, detailing the date and time of the event, the point that triggered the event, the reason code, and the recorded length pre- and post-event.
1.6.3.6 There will be no limit (other than that imposed by disk space) on the number of event capture files that can be accumulated.

1.6.3.7 Power Quality Event Capture should include a point viewer, which will allow users to analyze points from anywhere in the system, for a given event. The point viewer will also allow the user to select any event file and export it to Microsoft Excel for further analysis.

1.6.4 Event Data Recording

1.6.4.1 Event Data Recording application should 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

1.6.4.2 The event data should 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).

1.6.4.3 The system should record all logs from operators regardless if points are enabled as EDR.

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

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

1.6.4.5 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.

1.6.5 External Alarm Bell

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

1.6.5.2 It should 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.

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

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

1.6.6.3 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 on line frequency
- Accumulated time deviation (in milliseconds) between the reference time and the system time

1.6.6.4 The system should 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.

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

1.6.7 Fault Data Recorder

1.6.7.1 Fault Data Recorder will allow users to upload and record fault data from relays.

1.6.7.2 The editor should 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.

1.6.7.3 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.

1.6.7.4 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.

1.6.7.5 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.

1.6.7.6 The executive program of the Fault Data Recorder can be configured to operate in either Automatic Upload mode or in Manual Upload mode.
1.6.7.7 Additional to fault data, the system should include a COMTRADE viewer (license feature).

1.6.8 IED Wizard Templates

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

1.6.8.2 The user should 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.

1.6.8.3 The template should 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 should be automatically generated.

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

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

1.6.8.6 The vendor should 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.

1.6.9 Inter Control Center Protocol (ICCP)

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

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

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

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

1.6.9.5 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.

1.6.9.6 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.

1.6.9.7 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.

1.6.9.8 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.

1.6.9.9 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.

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

1.6.9.11 SBO for setpoints should be enforced.

1.6.9.12 The system supports Secure ICCP

1.6.10 Virtual RTU

1.6.10.1 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.

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

- Status
- Analog
- Accumulator
- Control
- Setpoint

1.6.10.3 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.

1.6.10.4 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.
1.6.10.5 Outbound Scaling factor should be supported.

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

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

1.6.10.8 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.

1.6.11 Interface to Microsoft Excel and Access

1.6.11.1 The system should support current and historical database access from clients running MS Excel. It should 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 should support redundant Host and automatically reconnect to the active Host upon failover. All current and historical tables and fields should be accessible through this interface.

1.6.11.2 For current data, the user should be able to select a database table, data fields within the table, and logic criteria (<, >, =, AND, OR) for point selection. In addition, the user should be able to browse for points and drag-drop them into the point selection dialog. The user should 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 should be able to optionally define a time interval at which the current data is automatically updated on the worksheet.

1.6.11.3 For Historical data, the user should be able to select points contained within a historical dataset. The user should 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 should be able to select data condition codes to be included with the samples. The user should 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.

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

1.6.12 Master/Slave Alarm Suppression

1.6.12.1 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.

1.6.12.2 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.
1.6.12.3 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.

1.6.12.4 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.

1.6.13 MultiSpeak

1.6.13.1 The Servers Editor should define links to other systems. The links should specify the type of interface, the communications ports or IP addresses used to access the other system, and other communication parameters.

1.6.13.2 MultiSpeak 5 should be supported.

1.6.13.3 Connectivity Import interface should import network connectivity data from GIS or Engineering Analysis into SCADA. The interface should:

- Parse the XML file that contains the connectivity data
- Import information relevant to SCADA connectivity database
- Discard layers in the GUI map containing previously imported data
- Add line sections to the map to correspond to the newly imported line sections.

1.6.14 MultiSpeak Network Model Import

1.6.14.1 DMS Network Model Import interface should import the full network model from GIS or Engineering Analysis into the ADMS. This supports:

- Section (instead of nodal)
- Full dump imports (instead of incremental)

1.6.14.2 The Import Configuration editor should have the ability to set up the Import parameters, including assignment of SCADA points to switch line sections.

1.6.14.3 The system must support the following function.

<table>
<thead>
<tr>
<th>Method</th>
<th>Direction</th>
<th>3.0</th>
<th>4.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>PingUrl</td>
<td>Sent</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PingUrl</td>
<td>Received</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>GetMethods</td>
<td>Sent</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>GetMethods</td>
<td>Received</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

1.6.15 MultiSpeak Dynamic GIS Viewer

1.6.15.1 The system supports Dynamic GIS Viewer interface that could publish analog and status point data to a Geographical Information System (GIS).
1.6.15.2 The system should support the following methods for sending and receiving analog and status point information.

<table>
<thead>
<tr>
<th>Method</th>
<th>Direction</th>
<th>3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetAllSCADAPoints</td>
<td>Received</td>
<td>✓</td>
</tr>
<tr>
<td>GetSCADAAnalogBySCADAPointID</td>
<td>Received</td>
<td>✓</td>
</tr>
<tr>
<td>GetSCADASTatusBySCADAPointID</td>
<td>Received</td>
<td>✓</td>
</tr>
<tr>
<td>SCADAAnalogChangedNotification</td>
<td>Sent</td>
<td>✓</td>
</tr>
<tr>
<td>SCADASTatusChangedNotification</td>
<td>Sent</td>
<td>✓</td>
</tr>
</tbody>
</table>

1.6.16 MultiSpeak Engineering Analysis

1.6.16.1 The system should support the Engineering Analysis interface that is capable of publishing analog and status point data to an Engineering Analysis (EA) system.

1.6.16.2 The system should support the ability to map SCADA points to the EA circuit elements specifying which SCADA points should be associated with which devices in the model.

1.6.16.3 The system should support SCADA analog values such as fault currents and feeder currents that can be used for such applications as fault location and load allocation.

1.6.16.4 The system should support the following methods for sending and receiving status and analog point information.

<table>
<thead>
<tr>
<th>Method</th>
<th>Direction</th>
<th>3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetAllSCADAPoints</td>
<td>Received</td>
<td>✓</td>
</tr>
<tr>
<td>GetSCADAAnalogBySCADAPointID</td>
<td>Received</td>
<td>✓</td>
</tr>
<tr>
<td>GetSCADASTatusBySCADAPointID</td>
<td>Received</td>
<td>✓</td>
</tr>
<tr>
<td>SCADAAnalogChangedNotification</td>
<td>Sent</td>
<td>✓</td>
</tr>
<tr>
<td>SCADASTatusChangedNotification</td>
<td>Sent</td>
<td>✓</td>
</tr>
</tbody>
</table>

1.6.17 MultiSpeak Load Management

The system should support the ability to use status points in the SCADA database to issue Load Shed and Power Factor control commands via the Load Management interface. The system should also:

- Enable operators to set up status points that drive these commands.
- Enable the Command Sequencing, Load Curtailment or Power Factor Control applications to set up the status points that drive these commands.

The system should support the following methods for load shedding and power factor control information.

<table>
<thead>
<tr>
<th>Method</th>
<th>Direction</th>
<th>3.0</th>
<th>4.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>InitiateLoadManagementEvent</td>
<td>Sent</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
1.6.18 MultiSpeak Outage Analysis

1.6.18.1 The system should support Outage Analysis interface that is capable of publishing analog and status point data to an Outage Management System (OMS).

1.6.18.2 The system should support the ability of the breaker operations reported by SCADA to be used by OMS to automatically create verified SCADA outage/restored records for such events.

1.6.18.3 The system should support the following methods for sending and receiving outage information.

<table>
<thead>
<tr>
<th>Method</th>
<th>Direction</th>
<th>3.0</th>
<th>4.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetAllSCADAPoints</td>
<td>Received</td>
<td>✓</td>
<td>NA</td>
</tr>
<tr>
<td>GetSCADAAnalogBySCADAPointID</td>
<td>Received</td>
<td>✓</td>
<td>NA</td>
</tr>
<tr>
<td>GetSCADASTatusBySCADAPointID</td>
<td>Received</td>
<td>✓</td>
<td>NA</td>
</tr>
<tr>
<td>SCADAAnalogChangedNotification</td>
<td>Sent</td>
<td>✓</td>
<td>NA</td>
</tr>
<tr>
<td>SCADASTatusChangedNotification</td>
<td>Sent</td>
<td>✓</td>
<td>NA</td>
</tr>
</tbody>
</table>

1.6.18.4 The client must choose the suitable versions and functions for their system

1.6.19 Network Database Access (NDA) API

1.6.19.1 The system should 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.

1.6.19.2 The system should 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.

1.6.19.3 The system should 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.

1.6.19.4 The system should provide the following functions for the NDA API:

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

1.6.20 Network Topology

1.6.21

1.6.21.1 The Network Topology application should 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.

1.6.21.2 The Network Topology application should 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 current 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 (Distribution Power Flow is required).

1.6.21.3 Current system configuration should 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 current status of breakers, switches, and other circuit elements. For areas that are energized, SCS also indicates where the network is paralleled or looped. When a circuit becomes de-energized, paralleled or looped, SCS should raise an alarm to alert the operator.

1.6.21.4 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). A feeder trace function allows multiple circuits to be highlighted in different colors.
1.6.21.5 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.

1.6.21.6 Incremental imports based on timestamps from GIS objects (from connectivity and service locations) should be supported. The system should include a maintenance utility to check network model integrity such as non-associated or connected transformers and phase correction, meters non-associated to transformers or phase mismatch and service locations with no meters, the customer associated to meters or meters that do not have customers.

1.6.21.7 ABC and RWB conventions are supported

1.6.21.8 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".

1.6.21.9 Loops should be prevented to be calculated in normally closed ties.

1.6.21.10 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".

1.6.21.11 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.

1.6.21.12 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.

1.6.21.13 Capability to insert and remove temporary devices such jumpers, cuts and grounds, mobile generators and transformers.

1.6.21.14 Multiple temporary cuts, jumpers, and switches should be supported on the same line section. Temporary devices should be supported in switch orders.

1.6.21.15 When transformers are imported, the system should assist in correcting wrong GPS coordinates, these coordinates can be defined in degree, minutes, seconds and fraction of seconds.
1.6.21.16 A report of inactive objects such as meters, customers, and transformers should be generated and the option to delete them should be available based on user privileges.

1.6.21.17 The system should support leading zeros when ID locations are imported.

1.6.21.18 Upon importing, the connectivity import should clearly indicate unsuccessful imports and log errors to a file.

1.6.21.19 When meter service address is blank upon connectivity import, an option to use customer billing address should be possible.

1.6.21.20 Transformers and service locations should be possible to be imported in CSV format.

1.6.21.21 The system should be able to import generators DER from GIS including Solar, Wind turbines and biomass generators.

1.6.22 OPC Client/Server

1.6.22.1 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.

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

- 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 periodically optionally refresh all points (all data poll)

1.6.23 Operations and Outage Accounting

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

1.6.23.2 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.

1.6.23.3 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.

1.6.23.4 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).

1.6.23.5 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.

1.6.23.6 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.

1.6.24 Remote Alarm Annunciation

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

1.6.24.2 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

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

1.6.24.4 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.

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

1.6.24.6 It should 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
1.6.24.7 Users may also specify:

- Annunciation time delay, so that if someone is in the building but not in the control room, he/she will have time to come back to the control room and respond to the alarm before someone is paged
- Re-annunciation time interval, such that if the alarm is not acknowledged after this time interval, the page will be re-issued

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

1.6.24.9 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.

1.6.25 SCADA Replicator

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

1.6.25.2 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.

1.6.25.3 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.

1.6.25.4 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.

1.6.25.5 Replicator automatically fails over to the current active SCADA host.

1.6.25.6 Replicator itself can be configured to be redundant.

1.6.25.7 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.

1.6.26 Simple Network Management Protocol (SNMP)

1.6.26.1 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
1.6.26.2 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.

1.6.26.3 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.

1.6.26.4 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.

1.6.26.5 SNMP should 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

1.6.27 Switch Order Preparation

1.6.27.1 Switch Order Preparation application includes both switches orders and guarantees (guarantees are also commonly known as clearances).

1.6.27.2 The Switch Order Preparation application should be accessed through the GUI.

1.6.27.3 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.

1.6.27.4 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.

1.6.28 Browser

1.6.28.1 Web Interface

- Web Interface should provide real-time SCADA information to users via a web browser, without the need for custom installation or maintenance.
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.

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.

By making use of SCADA Replicator, web server reproduces the SCADA database on a separate server thereby offloading the SCADA host(s).

Web Interface is an instant, out-of-the-box solution providing unparalleled ease of use and service for your information requirements.

Web Interface leverages your significant investment in GUI graphics by allowing the users to view the screens in a web browser.

The Network Topology Processor should be executed automatically in response to changes in the state of a network device that alters the connectivity of the network.

The Network Topology Processor should successfully execute for radial, networked and loop-type connectivity and should be able to identify those parts of the network that are de-energized for a particular network state.

The information provided by this application is used in the ADMS to highlight each individual feeder in the network by a distinctive color or depending on their energized and de-energized state as configured by the system administrator or selected by the operators.

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

The Network Topology Processor should be able to detect an islanding condition and to process each individual topology as an electrically connected island.

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.

1.6.28.2 Mobile Application

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, and Windows operating systems. The new simplified system of menus requires less memory and performs faster on mobile devices.
Tabular data is available for mobile devices running Apple iOS, Android, and Windows operating systems.

Graphical data is available for mobile devices supporting HTML5 and SVG - Apple iOS V10+, Android V3+, and Windows operating systems.

Mobile Application must support:
- Secure Access
- Session Expiration
- HTTPS for User Name 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

1.6.29 Support Servers (licensed applications)

1.6.29.1 Data Forwarding

1.6.29.2 There will be an interface available to forward real-time updates from the production system to any of the support servers – Operator Training Simulator (OTS), an offline editing system and Quality Assurance System (QAS). The production system can forward data to all of support systems simultaneously.

1.6.29.3 Upon initialization, Data Forwarding will send the current values for all status, analog and text points, tags and temporary devices in the production database. Afterward, only updates will be sent to the support servers. There will be an option to send all point events or only telemetered point events.

1.6.29.4 The interface to any of the support servers can be started or stopped at any time – this can be done directly from the operator GUI in case they wish to do a simulation or test based on the current data. The interface can be set to autostart as well.

1.6.29.5 Operator Training Simulator (OTS)

1.6.29.5.1 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

1.6.29.6 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.

1.6.29.7 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.

1.6.29.8 Screen and Project

1.6.29.9 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.

1.6.29.10 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.

1.6.29.11 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.

1.6.29.12 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.

1.6.29.13 Importing of the GIS connectivity model, transformers and service locations can be done through the OES then published to the production system.

1.6.29.14 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.
1.6.29.15 A record of all database edits and graphics files modified will be kept for each project.

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

1.6.29.17 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.

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

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

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

1.6.29.21 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 green
- In addition, the point control dialogs are further distinguished by green 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.

1.6.29.22 Quality Assurance System (QAS) Environment

1.6.29.23 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.

1.6.29.24 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 blue
- In addition, the point control dialogs are further distinguished by blue 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.
1.6.30 Distributed Energy Resources (DERs) and Distributed Energy Resources Management System (DERMS)

1.6.30.1 When DER are present or planned to be integrated on the customer premises, SCADA/ADMS provides multiple mechanism and integration stages as standalone solutions or as certified third-party integration. Users will be able to monitor and control those DER with remote capabilities and standardized communication mechanisms assuming the following criteria:

- DNP 3.0, Modbus RTU/TCP, IEC61850 and OPC are desirable communication standards to be used.
- Monitoring and control should not override local protection of the DER asset.
- Upon grid connection/disconnection control orders from SCADA, the remote DER protection settings should provide the synchronization sequence and grid connection safety to local assets and distribution grid.
- DER asset settings to handle lost of power and online modes should not be handled or controlled from the SCADA and are specific to the asset type, its capabilities and engineering settings.
- SCADA controls should override local control algorithms for grid stability.

1.6.30.2 The SCADA system provides the ability to import or manually populate the distribution network model to provide visibility to the asset type, capacity and current status when communication to the DER are available. When the connectivity to the DER asset is lost, SCADA should consider the asset capability for the various system calculations such as State Estimation and Power Flow.

1.6.30.3 In the GUI, by hovering on the dynamic object, a tooltip will provide DER information such as capacity and current status.

1.6.30.4 The system can support synchronous generators, induction generators and inverter-based generator. Support for Active and reactive power is available.

1.6.30.5 The ADMS engine is capable of supporting DER to DMS functions such as DES, DPF and VVO.

1.6.30.6 For Volt-Var Optimization the system can support synchronous and inverter-based generators.

1.6.30.7 The control of Distributed Generators for VVO support is done by the means of setpoints controlling active and reactive power and power factor to the target units.

1.6.30.8 The DG for VVO control should allow the following operation modes:

- Control by reactive power
- Control by reactive power
Control by power factor.

No control: Allow the DG to follow local load or grid objectives.

1.6.30.9 By third party Distributed Energy Resource Management System, the ADMS can provide support for Microgrid or islanded operation and Fleet management. Connectivity to a standard third-party provider is done by the means of a standardized API, MultiSpeak, or normalized communication protocols.

1.6.30.10 The ADMS can host DMS functions to support DERMS system such as Power Flow, Topology calculations and State Estimation or pass relevant data for DERMS modules to perform these functions. For Fleet or aggregated systems, the DERMS will perform control based on the ADMS results.

1.6.30.11 The ADMS for direct connected DER can provide AGC and Load forecasting functionality, when DER are aggregated on a third-party system, such system is responsible on the forecasting of production (generation) and loading, the third-party DERMS system should be able to provide such data for ADMS planning and system management. Such forecast should be programmed at intervals based on customer use cases.

1.6.30.12 For aggregated systems, the third-party solution should be able to provide reserve and schedule assists for dispatch based on end user needs (applicable to C&I customers) or on grid services, when collaborating to ADMS network constrains. The scheduling should be able to be performed at the asset or ADMS system level. Scheduled should be able to be scripted and program in recurring modes base on TOU, System demand needs or forecasting. Capabilities such as optimal resource dispatch, flexible scheduling, black start, asset planning and local AGC, manual dispatch, emergency override, load sharing, price signaling, fuel optimization among others, can be present at the third-party DERMS system and interface with the ADMS for optimal network operation.

1.6.30.13 By the means of the ADMS or other enterprise interfaces, the third-party DERMS system should be able to ingest price signaling and optimize resources for dispatch based on pricing on energy tariffs and dispatch resources based of pricing forecast. DLMP (distribution locational marginal price) can be calculated provided the formula and the ADMS is configured to supply projected distribution status at DLMP calculation intervals.

1.6.30.14 Supported third-party DERMS solutions are capable to be configured for two types of economic dispatch:

- Using system control functions in real time or
- by the means of a dispatch planner based on resources and load forecast

1.6.30.15 The system can provide local or the necessary API interfaces to reporting and analysis systems.

1.6.30.16 Support for local or cloud-hosted solution is available upon systems requirements and use cases.
Both ADMS and Third-party DERMS solution can be accessed for local control, control room operation or based on remote access, vendors and customers should work on defining local cybersecurity guidelines, access control and compliance to security standards such as NERC when applicable. An extensive set of access control based on user privileges, zone control, access control, two factor authentication and password encryption are available for the systems.