****

**City of Seattle**

**Seattle City Light**

**Request for Information #SCL2014-01**

**TITLE: Transmission Substation Management Console**

**Response Due Date – 4:00 p.m. PDT, May 19, 2014**

|  |  |
| --- | --- |
| **Schedule of Events** | **Date** |
| RFI Release date | April 21, 2014 |
| Vendor Questions Conference | April 30, 2014  9:00 – 10:30 a.m. PDT |
| Responses due | May 19, 2014  4:00 p.m. PDT |
| Respond to | Mike.Dozier@seattle.gov |

*The City reserves the right to modify this schedule at the City’s discretion. Notification of changes in the response due date would be posted on the City website or as otherwise stated herein.*

**Vendor responses must be submitted by email to:**

Mike Dozier, Project Manager

City of Seattle

Seattle City Light

Mike.Dozier@seattle.gov

This RFI is issued as a means of technical discovery and information gathering. This RFI is for planning purposes only and should not be construed as a solicitation nor should it be construed as an obligation on the part of the City to make any purchases. This RFI should not be construed as a means to pre-qualify vendors.

From the information provided by the respondents to the RFI, a determination will be made regarding any actual contracting through a procurement process. Any future contract that may be awarded must comply with City procurement requirements. The City of Seattle may utilize the results of this RFI in drafting a competitive solicitation (RFP) for the subject services/products/equipment; in determining that only one market-based solution exists and in initiating a procurement process for that solution; or in concluding that no adequate solution currently exists to meet its functional and technical requirements and that any effort at procurement must be deferred.

Participation in this RFI is voluntary and the City will not pay for the preparation of any information submitted by a respondent or for the City’s use of that information.

1. **Background.**

Seattle City Light (SCL), a department of the City of Seattle, is a municipally owned and operated electric utility which provides generation, transmission, and distribution services. City Light serves approximately 400,000 residential, commercial, and industrial customers in Seattle and adjacent jurisdictions, making it the 10th largest public electric utility in the United States, based on energy sales.

As part of its network, City Light maintains 16 transmission substations in the greater Seattle area. At each substation, City Light currently uses conventional remote terminal unit (RTU) technology to monitor digital and analog points and to control equipment from the System Operation Center (SOC). Schweitzer Engineer Laboratories (SEL) provides the standard relays; standard revenue meters are Schneider Ion 8650’s. There are no communications protocols used within substations. The RTUs link to the SOC via Telegyr 8979 protocol.

SCL intends to install a new, server-based communications and monitoring system (a substation management console or SMC) in each substation. The SMC is expected to consist of a console (“hardware”), operating system and communication protocols, and user interface (“software”) although the exact functions and relationships of these (and potentially other) components are subject to discovery via this RFI. The SMC will be acquired in order to facilitate the following:

1. Increased data availability from new Intelligent Electronic Devices (IEDs) such as digital meters and relays.
2. Improved alarm management by eliminating combined alarms while also creating smart alarms, programmed to determine and display the root cause of a problem, to reduce alarm flooding.
3. Increased reliability of the alarm system by replacing outmoded signaling devices with video displays.
4. Preparation for the implementation of “Smart Grid” technology such as distribution automation, advanced metering, and voltage control management systems.
5. Implementation of secure remote access to information from outside the station for both engineering and maintenance purposes.
6. Implementation of on-line condition monitoring.

SCL is currently in the process of updating its Energy Management System (EMS). SCL expects that the new SCADA protocol between the EMS and the stations will be DNP3.0, either IP-based or serial. A future option of using IEC61850 protocol for EMS communications is also desirable.

1. **Purpose of This Request for Information**

SCL is submitting this RFI in order to gain a better understanding of current transmission substation management console products and technologies, the companies which provide them, and the services those companies offer in order to design, install, support, and/or train SCL staff to support their systems. As a result of the information received, City Light may do one or more of the following:

* Request additional information, conduct follow-up meetings with some or all respondents, and/or request some or all respondents to demonstrate the capabilities of their systems;
* Request references from some or all respondents to enable City Light to better assess how the respondent’s system is functioning in production for utilities comparable to City Light;
* Continue with a competitive procurement (Request for Proposals, Invitation to Bid, or other City of Seattle procurement procedures) which will be available to all vendors regardless of whether they have responded to this RFI, but using information gained from the RFI responses to shape the procurement documents;
* Determine that only one qualified solution exists in today’s marketplace and initiate a process leading to the procurement of that solution;
* Determine that the available solutions are not currently adequate to meet City Light’s needs or are not affordable and therefore do nothing.

1. **Requirements.**

City Light expects to acquire dual (primary and back-up) substation management consoles for each substation. Each will be based on an appliance or other dedicated computing hardware platform at the substation which will gather information from a network of sensing devices (IEDs) within the substation and send that data to other computer systems outside the substation.

Functions are expected to include:

* Data concentration/protocol conversion as the IEDs are queried, data gathered, protocols converted, and information sent to the EMS
* Human/machine Interface (HMI) for managing the substation
* Security and reporting through access logging and control

City Light strongly prefers a single console to perform all three of these functions; however, if that is not technically practical, City Light will entertain solutions comprised of multiple components. City Light desires to purchase the computing hardware and software from a single vendor who will deliver the hardware loaded with required firmware and software.

City Light currently desires the SMC to meet the following functional and technical requirements:

1. **SCADA and Substation Automation**

The Substation Management Console should function as the substation SCADA gateway and data concentrator. It should be capable of interfacing and communicating with a wide variety of IEDs in the substation, such as RTUs, protection relays, meters, PLCs, sensors, event and fault recorders, etc. It should unify all operational data for the power system network and all non-operational data for analysis and planning purposes.

The SMC should function as a protocol converter. It should have a comprehensive suite of communication protocols for interfacing with enterprise or host systems such as the EMS and historical databases, as well as IEDs in substations. The SMC should have a library with, as a minimum, the following protocols:

Server protocols for forwarding data to a host system

• DNP3.0 (serial and TCP/IP)

• Modbus (serial and TCP/IP)

• OPC

Client protocols for acquiring data from downstream devices

• DNP3.0 (serial and TCP/IP)

• IEC-61850

• Modbus (serial and TCP/IP)

• SEL client

The SMC should enable the user to interface with the host system and field devices using any of the available protocols and exchange data via its database. It should be capable communicating to IEDs from various manufacturers via IEC-61850 protocol.

1. **Protection and Control Data Management**

The SMC should function as a data concentrator, acquiring operational information from the protective relays. It should be capable of integrating legacy relays from various manufacturers using industry standard protocols and specific relay vendor proprietary protocols, especially those from Schweitzer Engineering Labs, as those are the relays SCL currently uses. The SMC should also enable remote access to relays using their native software via virtual connection or pass through. It should support user defined, preset configurations of virtual connections to IEDs, simplifying remote access to the devices.

The SMC should enable users to upload files from the relays, including setting files, event files, fault and waveform files, etc. It should support the COMTRADE format for file transfer. It should also support manual or automatic file upload from IEDs to the SMC based on user defined triggers. It should be able to forward relay data, files and settings to the relay management software for archiving, monitoring, analyzing and planning.

1. **Remote Access for Engineering and Maintenance**

The SMC should support secure remote access to substation data, information, graphical interfaces, IEDs, and other subsystems and connected devices. Connection to IEDs should be made via virtual connection or pass through using the IED’s native software. It should have configuration tools for setting virtual connection parameters during system set up. The SMC should enable users with verified security approvals to easily view information from designated IEDs.

For IEDs that have only one serial communication port for both real-time data and maintenance purposes, the SMC should also be capable of communicating with these IEDs to exchange both real-time and non-operational data using the same communication port, or port binding.

The SMC should also support automatic retrieval of data files from IEDs based on user configurable settings. IED data files include sequence of events, faults, waveforms, history, logs, etc. It should also be capable of forwarding the IED files automatically to a central computer or server for storage and archiving.

1. **Human Machine Interface**

The SMC should have an integrated human machine interface (HMI) for presenting and displaying data and information to users. The SMC should support access from a client workstation normally located within the substation. It should support concurrent multiple user access.

The substation HMI should support the following overall features and functionalities:

* Graphical user interface
* Real-time and historical data processing
* Data collection from substation IEDs
* Automatic file retrieval and upload from IEDs
* Integrated cyber security features
* Redundant system architecture and failover switching
* Hardware platform independent
* Support for multiple resolutions of graphical displays to fit various types and sizes of monitors

The substation HMI should include the following components:

* Embedded real-time operating system
* Non-restricted HMI development tool kits
* Built-in maintenance and diagnostic tools
* Integration with the digital video monitoring system (see Subsection 7 below)

The HMI should support the following core functions:

* Graphically display a power circuit one-line diagram, emulate and display power system apparatus such as transformers, breakers, etc., and emulate and display substation IEDs such as protective relays
* Provide user definable and configurable objects and properties
* Provide support for HMI designs based on current recommended practices such as those found in the ASM Consortium’s guidelines, ISA Standard 101, and “The High Performance HMI Handbook” by Hollifield, Oliver, Nimmo, and Habibi
* Provide full support for ISA Standard 18.2, Alarm Management
* View, filter, and acknowledge alarms using a tabular view or custom annunciator displays
* Support user defined alarm schemes, including parent and child alarms, annunciation and acknowledgement, object colors, and trending of real time or historic data and events
* Provide the ability to display real time data without specific custom work
* Support user defined objects and properties, control properties, executable commands and programs, and zooming and panning capability within the graphical display
* Save objects and properties in a template library
* Support drawings and images imported from third-party software such Visio and media files

1. **IT and Cyber Security**

At a minimum the SMC should have cyber security features and functions that comply with the latest security definitions, measures and standards set out by the North America Electricity Reliability Corporation Critical Infrastructure Protection (NERC/CIP) standards, including the upcoming version 5 standards.

The SMC should be capable of operating independently with comprehensive cyber security features and functionalities, as well as operating in conjunction with remote access management, logging and other centralized security services. It should provide the following capabilities:

1. User Provisioning & Management

* System administrator definable native users and user groups with no requirement for connection to any remote or centralized directory service
* Management of native SMC user accounts via a standards based Open-LDAP service running natively on the SMC server(s).
* Ability to define and manage users and groups through a connection to an existing remote / centralized directory service such as Open-LDAP, RADIUS, or Active Directory.
* The option of provisioning a dedicated separate system running standards based Open-LDAP (not Active Directory) as part of the overall SMC system architecture would be considered so long as the design could be extended to provide such services centrally to all substations.
* Granular user account controls including but not limited to account aging, password aging, password complexity, and time and / or location based login restrictions.
* Central or distributed administrator tools for user provisioning and management

1. Access Control

* Ability to intercept, control, and log all access to HMI, IEDs, and other system components.
* Any and all access to the SMC system(s) must utilize the implemented authentication and authorization process.
* Support for strong authentication mechanisms including but not limited to multi-factor authentication.
* Ability to authenticate and authorize user access locally at SMC server.
* Ability to authenticate and authorize user access via central directory service(s).
* Ability to provide local access to IEDs through the SMC in the event of communication loss with the central directory service.
* Ability to provide audit trail through event logging of all user activities including but not limited to control execution or access of the HMI or IEDs.
* Ability to log all administrator actions on the SMC system(s).
* Ability to define custom logging criteria and alert events.
* Ability to monitor and log SMC system state information and events.
* Ability to collect and forward available Syslog and / or SNMP information from connected IEDs.
* Ability to generate activity reports for audit.
* Ability to forward log files and system event information to central logging and monitoring servers via Syslog and/or SNMP v3.

1. Data Security

* Integrated security functionality to block connections from undefined devices based on IP and / or MAC address.
* Data encryption options to secure all data exchange between devices and users.
* Support for SSH, SSL/TLS, and IPsec.
* All interactions with the SMC system(s) that utilize a web browser must support HTTPS
* Support secure file transfer by FTP and SFTP
* Provide anti-malware capability

1. **Integrated On-line Condition Monitoring**

The SMC should be capable of providing integrated on-line condition monitoring of power system apparatus in substations. The SMC should be capable of processing and managing this data for condition monitoring.

It should be capable of converting the data into useful information and displaying that information on the HMI, thereby enabling the optimization of operation and maintenance of the apparatus.

The SMC should be capable of interfacing to a historian or warehouse for archiving data.

It should also be capable of forwarding data to analytics and business applications such as PI Server historian and Oracle databases.

1. **Integrated Video Monitoring and Analytics**

The SMC should have the capability to interface with a digital video recorder (DVR). While the DVR system is an independent sub-system, the SMC should be the user interface and access point for launching and controlling the DVR server. The SMC should be capable of acquiring discrete alarms, as well as video data, from the DVR system and presenting them on a video display with appropriate resolution. The selected SCMS vendor may be required to integrate and support a third party application or applications to enable video monitoring functionality.

1. **Redundant System Architecture**

The SMC should be fully redundant, with support for the following technologies:

* Redundant server architecture
* Serial and Ethernet channel redundancy
* Synchronized databases between the two SMC servers
* Hot standby failover switching
* User definable multiple triggers for failover switching

1. **Programmable Logic**

The SMC should have an integrated, programmable logic application that enables users to customize automation processes, data conversion and computation, animation displays, and other automation needs. The user programming interface should meet IEC-61131-3 standards.

1. **Time Synchronization**

The SMC should have an internal real-time clock, and should be capable of performing time synchronization. The following time synchronization methods should be supported:

* IRIG-B
* IEEE 1588 V2
* NTP (client and server)

The SMC should be capable of receiving a time synchronization signal from a host system via a protocol such as DNP3.0, and synchronizing its internal clock to that signal. It should also be able to synchronize its internal clock directly from a GPS clock using one of the protocols listed above. It should be able to distribute time synchronization signals to IEDs via serial communication channels or over Ethernet using IEEE 1588 V2 protocol.

1. **Operating System, Databases, and Software**

The SMC should utilize some variant of Linux as the base operating system for ease in maintaining security compliance.

The SMC should have real-time and historical databases for storing information. The databases should support SQL queries and programming, and be ODBC compliant for data export.

The SMC application software should be integrated with the SMC computer hardware and Linux operating system to form an embedded SMC system.

The SMC must have the ability to use different hardware from multiple manufacturers. Since the SMC must meet the requirements of an integrated embedded system, and be transportable to various hardware platforms, custom integration of SMC software and hardware is acceptable when a new hardware platform is selected. However, this should be a one time engineering and software development effort. Thereafter, the user should be able to install the SMC software on the hardware selected.

1. **SMC Hardware Platform**

The SMC should be delivered by the vendor loaded on a hardware platform. The hardware should meet the following requirements:

* Utility substation hardened, in conformance with IEC 61805-3, IEC 61850-3, and IEEE 1613
* High performance industrial grade CPU
* On-board flash memory
* Scalable on-board data storage using compact flash (CF) or solid state disc (SSD) technologies
* Serial communication channels, configurable for RS-232/422/485
* RS-232 ports
* RS-232/422/485 ports
* RS-232 console port
* At least 3 each 10/100/1000 Base T Ethernet ports
* USB ports
* Interface to LCD display, keyboard and mouse
* IRIG-B input and output connections

1. **User Configuration and Maintenance Interface**

The SMC should have a utility software application for system configuration and maintenance. This software should have a graphical user interface. All setup, configuration, engineering, development, maintenance, testing, and troubleshooting tools should be in one software package. Users should be able to run this utility software and launch various modules or tools as needed.

The configuration and maintenance utility software should have the following characteristics and features:

* Support on-line or off-line configuration and development work
* IED database, configuration, and logic import utilities
* Graphical user interface
* Library to store pre-configured IEDs, HMI screens, and other objects
* Does not require use of Linux OS commands
* Modular, intuitive, and easy to use
* Built-in real-time data communications monitor
* Built-in protocol translator
* All actions executed in the utility software against any SMC server must be logged in the SMC server
* Access to the SMC server for users of the utility software must meet the authentication and authorization requirements specified in Section 5, including granular access control applied to utility software functionality
* No license restrictions on installation

1. **Submittals**

If you have a product that you feel will meet our needs please complete and submit, via email, [**Attachment A,** **Specifications Checklist and Vendor Information**.](#AttachmentA)  You may include with **Attachment A** any additional information in pdf format which you believe Seattle City Light should consider in pursuing a Substation Management Console System. City Light does not promise to read or consider all information which a vendor may submit.

1. **Questions**

Questions shall be submitted in writing, by e-mail only, tothe **Project Manager:**

**Name:** Mike Dozier

**E-Mail:** [Mike.Dozier@seattle.gov](mailto:Mike.Dozier@seattle.gov)

In addition, City Light will conduct a Vendor Questions Conference at the date and time identified on page 1 of this RFI. If you are interested in participating, please email Mike Dozier ([Mike.Dozier@seattle.gov](mailto:Mike.Dozier@seattle.gov)) at least 24 hours prior to the Vendor Questions Conference so that he can provide you with the phone number and dial-in instructions.

## Receiving Answers and addenda

Any addenda and notices, as well as answers to Vendors’ questions, will be posted on the City’s website at: <http://www.seattle.gov/purchasing/>. The City will make efforts to provide courtesy notices, reminders, addenda and similar announcements directly to any interested vendors known by the City. Notwithstanding efforts by the City to provide such notice to such known vendors, it remains the obligation and responsibility of the Vendor to learn of any addenda, responses, or notices issued by the City. Such efforts by the City to provide notice or to make it available do not relieve the Vendor from the sole obligation for learning of such material.

## Response Date and Location

###### Vendors should submit their Specification Checklist to the Project Manager no later than the date and time given on page 1.

1. The Subject Line of your email should be “**Substation Management Console, Specifications Checklist**”. This is important to insure proper handling of your response.
2. The Vendor has full responsibility to ensure their response arrives to the Project Manager before the deadline. That being said, the City, at its sole discretion and convenience may choose to review responses that arrive within a reasonable time after the deadline.

## 8. Proprietary Material.

## The State of Washington’s Public Records Act (Release/Disclosure of Public Records)

Under Washington State Law (reference RCW Chapter 42.56, the ***Public Records Act***) all materials received or created by the City of Seattle are considered ***public records***. These records include but are not limited to bid or proposal submittals, agreement documents, contract work product, or other bid material.

The State of Washington’s Public Records Act requires that public records must be promptly disclosed by the City upon request unless that RCW or another Washington State statute specifically exempts records from disclosure. Exemptions are narrow and explicit and are listed in Washington State Law (Reference RCW 42.56 and RCW 19.108).

Respondents must familiarize themselves with the Washington State Public Records Act and the limits of record disclosure exemptions. For more information, visit the Washington State Legislature’s website at <http://www1.leg.wa.gov/LawsAndAgencyRules>).

***If you have any questions about disclosure of the records you submit with your informational material, please contact the RFI Coordinator.***

## Marking Your Records Exempt from Disclosure (Protected, Confidential, or Proprietary)

As mentioned above, all City of Seattle offices (“the City”) are required to promptly make public records available upon request. However, under Washington State Law some records or portions of records are considered legally ***exempt from disclosure*** and can be withheld. A list and description of records identified as exempt by the Public Records Act can be found in RCW 42.56 and RCW 19.108.

If you believe any of the records you are submitting to the City as part of your informational material are exempt from disclosure, you can request that they not be released before you receive notification. To do so, you must complete the City Non-Disclosure Request Form (“the Form”) included below. You should very clearly and specifically identify each record and the exemption(s) that may apply.



The City will **not** withhold materials from disclosure simply because you mark them with a document header or footer, page stamp, or a generic statement that a document is non-disclosable, exempt, confidential, proprietary, or protected. Do not identify an entire page as exempt unless each sentence is within the exemption scope; instead, identify paragraphs or sentences that meet the specific exemption criteria you cite on the Form. Only the specific records or portions of records properly listed on the Form will be protected and withheld for notice. All other records will be considered fully disclosable upon request.

If the City receives a public disclosure request for any records you have properly and specifically listed on the Form, the City will notify you in writing of the request and will postpone disclosure. While it is not a legal obligation, the City, as a courtesy, will allow you up to ten business days to file a court injunction to prevent the City from releasing the records (reference RCW 42.56.540). If you fail to obtain a Court order within the ten days, the City may release the documents.

The City will **not** assert an exemption from disclosure on your behalf. If you believe a record(s) is exempt from disclosure you are obligated to clearly identify it as such on the Form and submit it with your solicitation. Should a public record request be submitted to the Department of Finance and Administrative Services for that (those) record(s) you can then seek an injunction under RCW 42.56 to prevent release. By submitting a response to this Request for Information, Respondent acknowledges this obligation; and also acknowledges that the City will have no obligation or liability to the proposer if the records are disclosed.

## 9. Cost of Preparing Responses

The City will not be liable for any costs incurred by the Respondent in the preparation and presentation of information submitted in response to this RFI including, but not limited to, costs incurred in connection with the Respondent’s participation in demonstrations and the informational conference.

**Attachment A**

**Specifications Checklist**

Company Name:

Product Name:

Contact Name, Title:

Contact Phone:

Contact Email:

Please check the Yes or No column to let us know whether your product can meet the functional and technical specifications below. If your product partially meets the specification, or if you think the specification is not relevant or appropriate, please use the Comments field to explain. You may also use a separate document to identify questions, concerns, or suggestions. If using a separate document, please try to reference the specifications by number so that there is no confusion about which item or items you are referring to.

Please send your completed form and any additional information via email to the address specified on page 1 of this RFI. Thank you for responding!

| **#** | **Feature or Function** | **Yes** | **No** | **Comments** |
| --- | --- | --- | --- | --- |
|  | 1. **SCADA and Substation Automation** |  |  |  |
|  | The Substation Management Console (SMC) should: |  |  |  |
| 1.1 | function as the substation SCADA gateway and data concentrator. |  |  |  |
| 1.2 | be capable of interfacing and communicating with a wide variety of IEDs in the substation, such as RTUs, protection relays, meters, PLCs, sensors, event and fault recorders, etc. |  |  |  |
| 1.3 | unify all operational data for the power system network and all non-operational data for analysis and planning purposes. |  |  |  |
|  | The SMC should: |  |  |  |
| 1.4 | function as a protocol converter. |  |  |  |
| 1.5 | have a comprehensive suite of communication protocols for interfacing with enterprise or host systems, as well as IEDs in substations. |  |  |  |
|  | have a library with, as a minimum, the following protocols: |  |  |  |
|  | Server protocols for forwarding data to a host system |  |  |  |
| 1.6 | • DNP3.0 (serial and TCP/IP) |  |  |  |
| 1.7 | • Modbus (serial and TCP/IP) |  |  |  |
| 1.8 | • OPC |  |  |  |
|  | Client protocols for acquiring data from downstream devices |  |  |  |
| 1.9 | • DNP3.0 (serial and TCP/IP) |  |  |  |
| 1.10 | • IEC-61850 |  |  |  |
| 1.11 | • Modbus (serial and TCP/IP) |  |  |  |
| 1.12 | • SEL client |  |  |  |
|  | The SMC should: |  |  |  |
| 1.13 | enable the user to interface with the host system and field devices using any of the available protocols and exchange data via its database. |  |  |  |
| 1.14 | be capable communicating to IEDs from various manufacturers via IEC-61850 protocol. |  |  |  |
|  | 1. **Protection and Control Data Management** |  |  |  |
|  | The SMC should: |  |  |  |
| 2.1 | function as a data concentrator, acquiring operational information from the protective relays. |  |  |  |
| 2.2 | be capable of integrating various legacy relays from various manufacturers using industry standard protocols and specific relay vendor proprietary protocols. |  |  |  |
| 2.3 | enable remote access to relays using their native software via virtual connection or pass through. |  |  |  |
| 2.4 | support user defined, preset configurations of virtual connections to IEDs, simplifying remote access to the devices. |  |  |  |
| 2.5 | enable users to upload files from the relays, including setting files, event files, fault and waveform files, etc. |  |  |  |
| 2.6 | support the COMTRADE format for file transfer. |  |  |  |
| 2.7 | support manual or automatic file upload based on user defined triggers. |  |  |  |
| 2.8 | be capable of interfacing to other protection relay database management and analytics software. |  |  |  |
| 2.9 | be able to forward relay data, files and settings to the relay management software for archiving, monitoring, analyzing and planning. |  |  |  |
|  | 1. **Remote Access for Engineering and Maintenance** |  |  |  |
|  | The SCM should |  |  |  |
| 3.1 | support secure remote access to substation data, information, graphical interfaces, IEDs, and other subsystems and connected devices. Connection to IEDs should be made via virtual connection or pass through using the IED’s native software. |  |  |  |
| 3.2 | have configuration tools for setting virtual connection parameters during system set up. |  |  |  |
| 3.3 | enable users to easily launch IED software and automatically connect to the designated IED. |  |  |  |
| 3.4 | be capable of communicating to IEDs for both real-time and non-operational data using the same communication port, or port binding. |  |  |  |
| 3.5 | support automatic retrieval of data files from IEDs based on user configurable settings. IED data files include sequence of events, faults, waveforms, history, logs, etc. |  |  |  |
| 3.6 | be capable of forwarding the IED files automatically to a central computer or server for storage and archiving. |  |  |  |
|  | 1. **Human Machine Interface (HMI)** |  |  |  |
| 4.1 | The SMC should have an integrated HMI for presenting and displaying data and information to users. |  |  |  |
| 4.2 | The SMC should support access from a client workstation located within the substation. |  |  |  |
| 4.3 | The HMI should support concurrent multiple user access. |  |  | How many concurrent users will your proposed HMI support? |
|  | The HMI should support the following overall features and functionalities: |  |  |  |
| 4.4 | * Graphical user interface |  |  |  |
| 4.5 | * Support for multiple resolutions of graphical displays to fit various types and sizes of monitors |  |  |  |
| 4.6 | * Real-time and historical data processing |  |  |  |
| 4.7 | * Data collection from substation IEDs |  |  |  |
| 4.8 | * Automatic file retrieval and upload from IEDs |  |  |  |
| 4.9 | * Integrated cyber security features |  |  |  |
| 4.10 | * Redundant system architecture and failover switching |  |  |  |
| 4.11 | * Hardware platform independence |  |  |  |
|  | The substation HMI should include the following components: |  |  |  |
| 4.12 | * Embedded real-time operating system |  |  |  |
| 4.13 | * Non-restricted HMI development tool kits |  |  |  |
| 4.14 | * Built-in maintenance and diagnostic tools |  |  |  |
| 4.15 | * Integration with the digital video monitoring system (see Subsection 7 below) |  |  |  |
|  | The HMI should support the following core functions: |  |  |  |
| 4.16 | * Graphically display a power circuit one-line diagram, emulate and display power system apparatus such as transformers, breakers, etc., and emulate and display substation IEDs such as protective relays |  |  |  |
| 4.17 | * Provide user definable and configurable objects and properties |  |  |  |
| 4.18 | * Provide support for HMI designs based on current recommended practices such as those found in the ASM Consortium’s guidelines, ISA Standard 101, and “The High Performance HMI Handbook” by Hollifield, Oliver, Nimmo, and Habibi |  |  |  |
| 4.19 | * Provide full support for ISA Standard 18.2, Alarm Management |  |  |  |
| 4.20 | * View, filter, and acknowledge alarms using a tabular view or custom annunciator displays |  |  |  |
| 4.21 | * Support user defined alarm schemes, including parent and child alarms, annunciation and acknowledgement, object colors, and trending of real time or historic data and events |  |  |  |
| 4.22 | * Provide the ability to display real time data without specific custom work |  |  |  |
| 4.23 | * Support user defined objects and properties, control properties, executable commands and programs, and zooming and panning capability within the graphical display |  |  |  |
| 4.24 | * Save objects and properties in a template library |  |  |  |
| 4.25 | * Support drawing and images imported from third-party software such Visio and media files |  |  |  |
|  | 1. **IT and Cyber Security** |  |  |  |
| 5.1 | The SMC should have cyber security features and functions that comply with the latest security definitions, measures and standards set out by the North America Electricity Reliability Corporation Critical Infrastructure Protection (NERC/CIP) standards, including the upcoming version 5 standards. |  |  |  |
| 5.2 | The SMC should be capable of operating independently with comprehensive cyber security features and functionalities, as well as operating in conjunction remote access management, logging and other centralized security services. |  |  |  |
|  | The SMC should provide the following capabilities: |  |  |  |
|  | 1. User Management |  |  |  |
| 5.3 | * System administrator definable users and user groups with no requirements for connection to remote or centralized directory service. |  |  |  |
| 5.4 | * Management of native SMC user accounts via standards based Open-LDAP service running natively on the SMC server(s). |  |  |  |
| 5.5 | * Ability to define and manage users and groups through a connection to an existing remote / centralized directory service such as Open-LDAP, RADIUS, or Active Directory |  |  |  |
| 5.6 | * The option of provisioning a dedicated separate system running standards based Open-LDAP (not Active Directory) as part of the overall SMC system architecture would be considered so long as the design could be extended to provide such services centrally to all substations |  |  |  |
| 5.7 | * Granular user account controls including but not limited to account aging, password aging, password complexity, and time and / or location based login restrictions |  |  |  |
| 5.8 | * Central or distributed administrator tools for user provisioning and management |  |  |  |
|  | 1. Access Control |  |  |  |
| * 5.9 | * Ability to intercept, control, and log all access to HMI, IEDs, and other system components |  |  |  |
| 5.10 | * Any and all access to the SMC system(s) must utilize the implemented authentication and authorization process |  |  |  |
| 5.11 | * Support for strong authentication mechanisms including but not limited to multi-factor authentication |  |  |  |
| 5.12 | * Ability to authenticate and authorize user access locally at SMC server |  |  |  |
| 5.13 | * Ability to authenticate and authorize user access via central security server |  |  |  |
| 5.14 | * Ability to provide local access to IEDs through the SMC in the event of communication loss with the central directory service |  |  |  |
| 5.15 | * Ability to provide audit trail through event logging of all user activities including but not limited to control execution or access of the HMI or IEDs |  |  |  |
| 5.16 | * Ability to log all administrator actions on the SMC system(s). |  |  |  |
| 5.17 | * Ability to define custom logging criteria and alert events SMC |  |  |  |
| 5.18 | * Ability to monitor and log SMC system state information and events |  |  |  |
| 5.19 | * Ability to collect and forward available Syslog and / or SNMP information from connected IEDs |  |  |  |
| 5.20 | * Ability to generate activity reports for audit |  |  |  |
| 5.21 | * Ability to forward log file and system event information to central logging and monitoring servers via Syslog and/or SNMP v3 |  |  |  |
|  | 1. Data Security |  |  |  |
| 5.22 | * Integrated security functionality to block connections from undefined devices based on IP and / or MAC address |  |  |  |
| 5.23 | * Data encryption options to secure all data exchange between devices and users |  |  |  |
| 5.24 | * Support for SSH, SSL/TLS, and IPsec |  |  |  |
| 5.25 | * All interactions with the SMC system(s) that utilize a web browser must support HTTPS |  |  |  |
| 5.26 | * Support secure file transfer by FTP and SFTP |  |  |  |
| 5.27 | * Provide anti-malware capability |  |  |  |
|  | 1. **Integrated On-Line Condition Monitoring** |  |  |  |
|  | The SCM should be capable of |  |  |  |
| 6.1 | providing integrated on-line condition monitoring of power system apparatus in substations. |  |  |  |
| 6.2 | processing and managing this data for condition monitoring. |  |  |  |
| 6.3 | converting the data into useful information and displaying that information on the HMI, thereby enabling the optimization of operation and maintenance of the apparatus. |  |  |  |
| 6.4 | interfacing to a historian or warehouse for archiving data. |  |  |  |
| 6.5 | forwarding data to analytics and business applications. |  |  |  |
|  | 1. **Integrated Video Monitoring and Analytics** |  |  |  |
|  | The SCM should be capable of |  |  |  |
| 7.1 | interfacing with a digital video recorder (DVR). While the DVR system is an independent sub-system, the SMC should be the user interface and access point for launching and controlling the DVR server. |  |  |  |
| 7.2 | acquiring discrete alarms, as well as video data, from the DVR system and presenting them on a video display with appropriate resolution. |  |  |  |
|  | 1. **Redundant System Architecture** |  |  |  |
|  | The SMC should be fully redundant, with support for the following technologies: |  |  |  |
| 8.1 | * Redundant server architecture |  |  |  |
| 8.2 | * Serial and Ethernet channel redundancy |  |  |  |
| 8.3 | * Synchronized databases between the two SMC servers |  |  |  |
| 8.4 | * Hot standby failover switching |  |  |  |
| 8.5 | * User definable multiple triggers for failover switching |  |  |  |
|  | 1. **Programmable Logic** |  |  |  |
| 9.1 | The SMC should have an integrated, programmable logic application that enables users to customize automation processes, data conversion and computation, animation displays, and other automation needs. |  |  |  |
| 9.2 | The user programming interface should meet IEC-61131-3 standards. |  |  |  |
|  | 1. **Time Synchronization** |  |  |  |
|  | The SCM should |  |  |  |
| 10.1 | have an internal real-time clock, and should be capable of performing time synchronization. |  |  |  |
|  | support the following time synchronization methods: |  |  |  |
| 10.2 | * IRIG-B |  |  |  |
| 10.3 | * IEEE 1588 V2 |  |  |  |
| 10.4 | * NTP (client and server) |  |  |  |
| 10.5 | be capable of receiving a time synchronization signal from a host system via a protocol such as DNP3.0, and synchronizing its internal clock to that signal. |  |  |  |
| 10.6 | be able to synchronize its internal clock directly from a GPS clock using one of the protocols listed above. |  |  |  |
| 10.7 | be able to distribute time synchronization signals to IEDs via serial communication channels or over Ethernet using IEEE 1588 V2 protocol. |  |  |  |
|  | 1. **Operating System, Databases, and Software** |  |  |  |
| 11.1 | The SMC should utilize the Linux operating system. |  |  |  |
| 11.2 | The SMC should have real time and historical databases for storing information. |  |  |  |
| 11.3 | The databases should support SQL queries and programming, and be ODBC compliant for data export. |  |  |  |
| 11.4 | The SMC application software should be integrated with the SMC computer hardware to form an embedded SMC system. |  |  |  |
|  | The SMC should |  |  |  |
| 11.5 | have the ability to use different hardware from multiple manufacturers. |  |  | Please specify the hardware platforms on which your SMC operates. |
| 11.6 | Custom integration of SMC software and hardware is acceptable when a new hardware platform is selected; however, this should be a one time engineering and software development effort. Thereafter, the user should be able to install the SMC software on the hardware selected. |  |  |  |
|  | 1. **SMC Hardware Platform** |  |  |  |
| 12.1 | The SMC should be delivered by the vendor loaded on a hardware platform. |  |  |  |
|  | The hardware should meet the following requirements: |  |  |  |
| 12.2 | * Utility substation hardened, in conformance with IEC 61805-3, IEC 61850-3, and IEEE 1613 |  |  |  |
| 12.3 | * High performance industrial grade CPU |  |  |  |
| 12.4 | * On-board flash memory |  |  |  |
| 12.5 | * Scalable on-board data storage using compact flash (CF) or solid state disc (SSD) technologies |  |  |  |
| 12.6 | * Serial communication channels, configurable for RS-232/422/485 |  |  |  |
| 12.7 | * RS-232 ports |  |  | Number of ports: |
| 12.8 | * RS-232/422/485 ports |  |  | Number of ports: |
| 12.9 | * 1 RS-232 console port |  |  |  |
| 12.10 | * At least 3 each 10/100/1000 Base T Ethernet ports |  |  |  |
| 12.11 | * USB ports |  |  | Number of ports: |
| 12.12 | * Interface to LCD display, keyboard and mouse |  |  |  |
| 12.13 | * IRIG-B input and output jacks |  |  |  |
|  | 1. **User Configuration and Maintenance Interface** |  |  |  |
| 13.1 | The SMC should have a utility software application for system configuration and maintenance. |  |  |  |
| 13.2 | All setup, configuration, engineering, development, maintenance, testing, and troubleshooting tools should be in one software package. |  |  |  |
|  | The configuration and maintenance utility software should have the following characteristics and features: |  |  |  |
| 13.3 | * Support on-line or off-line configuration and development work |  |  |  |
| 13.4 | * IED database, configuration, and logic import utilities |  |  |  |
| 13.5 | * Graphical user interface |  |  |  |
| 13.6 | * Library to store pre-configured IEDs, HMI screens, and other objects |  |  |  |
| 13.7 | * Does not require use of Linux OS commands |  |  |  |
| 13.8 | * Modular, intuitive, and easy to use |  |  |  |
| 13.9 | * Built-in real-time data communications monitor |  |  |  |
| 13.10 | * Built-in protocol translator |  |  |  |
| 13.11 | * No license restrictions on installation |  |  |  |
| 13.12 | * All actions executed in the utility software against any SMC server are logged in the SMC server |  |  |  |
| 13.13 | * Access to the SMC server for users of the utility software meet the authentication and authorization requirements specified in Section 5, including granular access control applied to utility software functionality |  |  |  |
|  | 1. **General System Information** |  |  |  |
| 14.1 | Please provide an overview of your SMC solution, including hardware, software, highlighting any major differentiating qualities or characteristics. |  |  |  |
| 14.2 | Please briefly describe the process for configuring and implementing your SMC. |  |  |  |
| 14.3 | Please identify major electric utilities which deploy your SMC in their substations; it is not necessary to provide contact information for these utilities at this time. |  |  |  |
|  | 1. **Pricing Information** |  |  |  |
| 15.1 | Please provide pricing information for your SMC, configured as you have described it herein. **This is not a bid;** this information is solely for project budgeting purposes and price ranges are acceptable. |  |  |  |
|  |  |  |  |  |