

1. Scope

This specification describes the features and specifications of the SMP Gateway, as part of Eaton's Cooper Power Systems Substation Automation solution. The SMP Gateway is designed to work as a standalone product or with complement product such as Yukon IMS, Yukon Visual T&D and the SMP I/O.

2. Applicable Standards

The vendor shall have implemented an ISO 9001 certified Quality Management System.

3. Hardware Features

3.1. Form factor

3.1.1. The product shall be available in different form factor the fit the application. The following form factors are required: chassis / wall-mount.

3.2. Power Supply

3.2.1. The product shall have option for high voltage (AC/DC) and low voltage (DC) power supply.

3.3. Communication interfaces

3.3.1. The product shall have at least two independent 100Mb Ethernet ports in all models.

3.3.2. The product shall have a minimum of 4 serial ports

3.3.3. The product shall have a USB port on the front panel for maintenance purposes.

3.4. Time synchronization

3.4.1. The product shall have option for modulated IRIG-B input

3.5. Type tests and Certifications

3.5.1. The product shall be compliant to IEC 61850-3 class 3K7 (minimum) for climatic environmental conditions.

3.5.2. The product shall have an operating temperature of -40° to 85° Celcius.

3.5.3. The product shall be compliant to IEC 61850-3 class 3M6 (minimum) for mechanical environmental conditions.

3.5.4. The product shall be compliant to IEEE Std 1613™-2009 standard class 2 (minimum). All communication port types should comply.

3.5.5. The product shall have a CB Scheme certification/report for electrical security.

3.5.6. The product shall have CE Marking for low voltage electrical equipment.

3.5.7. The product shall have a CSA/UL certification.

3.5.8. The product shall be RoHS compliant.

3.5.9. The product shall be WEEE compliant.

4. Software Features

4.1. Protocols and Data concentration

4.1.1. The product shall support most industry standard protocols for gathering data from IEDs:

- DNP3 (IEEE Std 1815™-2012 standard) – including Secure Authentication V5
- IEC 61850 (including GOOSE)
- IEC 60870-5-101/103/104
- ICCP
- MODBUS
- IEEE Std C37.118™-2005 standard (synchrophasor)
- IEC 62056
- ABB SPABUS
- ABB Standard Ten Byte
- Algodue
- Areva Courier
- Beckwith
- BlueTree
- Conitel
- GE D.20 LAN (I/O modules)
- GE EGD (Ethernet Global Data)
- GE Syprotec (Hydran)
- Harris 5000/6000
- Hathaway
- Landis&Gyr (LG8979)
- Mehta Tech
- Morgan Sheffer Calisto
- Motorola MDAC
- Opto 22 (Optomux)
- PG&E (Cooper 2179)
- Schneider ION
- SEL Faster Meter
- Valmet (Tejas)

4.1.2. The product shall support most industry standard protocols for sending data to control centers or enterprise applications:

- DNP3 (IEEE Std 1815™-2012 standard) – including Secure Authentication V5
- IEC 61850
- IEC 60870-5-101/104
- ICCP
- OSISoft PI
- MODBUS
- IEEE Std C37.118™-2005 standard (synchrophasor)
- Conitel
- Harris 5000/6000
- GE EGD (Ethernet Global Data)
- Landis&Gyr (LG8979)
- SES-92

4.2. Event files retrieval

- 4.2.1. The product shall be able to retrieve event files (oscillography, SOE, fault records) from all the major IED vendors :
- SEL
 - GE
 - Areva
 - ABB
 - Siemens
 - ABB
 - Schneider
- 4.2.2. The product shall be able to retrieve event files (oscillography, SOE, fault records) using the following protocols:
- FTP
 - DNP3 file transfer
 - IEC 61850 file transfer
 - IEC 60870-5-103 file transfer
- 4.2.3. The product shall be able to act as a local repository for event files. It shall have sufficient non-volatile memory to store retrieved event files of a typical substation for about 1 month (up to 10,000 event files)
- 4.2.4. The product shall offer an easy way to browse and download the event files stored in its memory.

4.3. Security

- 4.3.1. The product shall implement cyber security regarding access, operation, configuration, firmware revision and data retrieval as defined by IEEE Std 1686™-2007 standard:
- Electronic access control :
 - Major functions have associated access level or permissions
 - Management of users and groups with associated permissions
 - System access management, include system lockup upon failed access attempts
 - Strong password enforcement
 - Audit trail :
 - At least 2048 entries for security specific logs
 - Other type of log entry shall not interfere with security logs
 - Supervisory monitoring and control:
 - Alarms sent to SCADA when authentication failure are detected
 - Ability to enable/disable remotely any passthrough access
 - Configuration software:
 - Distinct permissions allows to :
 - View device settings
 - Change device settings
 - Manage username/passwords
 - Communication port access
 - All communication ports shall be configurable. It shall be possible to disable all communication ports, on a port by port basis.
- 4.3.2. Firmware quality assurance:
- 4.3.3. All product components shall be digitally signed by the manufacturer.
- 4.3.4. The product shall provide secure passthrough access substation IEDs.

4.3.5. The product shall tie into enterprise level software allowing for :

- Central user account management
- IED configuration management
- IED event processing
- IED password management

4.3.6. The product shall implement secure communication networks as defined by IEC 62351-3. This shall apply to all remote communications links, including maintenance tools and SCADA protocols.

4.3.7. The product shall support TLS 1.2 with AES 256 bits encryption, with the possibility to use older encryption protocols to ensure compatibility with legacy devices or systems.

4.3.8. The product shall implement secure SCADA protocols as defined by IEC 62351-5. This shall include DNP3 Secure Authentication and ICCP Secure.

4.3.9. The product shall support X.509 certificates for authentication and encryption key management.

4.3.10. System logs shall be retrieved using a standard system such as Syslog.

4.3.11. The product shall have a built-in firewall.

4.3.12. Continuous system scan ensures only digitally signed components are running on the product.

4.4. **Configuration Tools**

4.4.1. The configuration tool shall allow off-line configuration of the product.

4.4.2. The configuration tool shall be template driven.

4.4.3. The configuration tool shall have import/export capabilities in Excel compatible format.

4.4.4. The configuration tool shall support copy/paste from/to Excel spreadsheet.

4.4.5. The configuration tool shall have import/export capabilities for IEC 61850 master and slave protocols (.icd files).

4.4.6. The configuration tool shall have import/export capabilities for IEEE Std 1815™-2012 standard (DNP3) master and slave protocols (XML format).

4.4.7. The configuration toolset shall support versioning.

4.4.8. The configuration toolset shall be backward compatible – it shall allow the configuration of older firmware versions and conversion to newer version.

4.4.9. The configuration tool shall include a configuration parameter validation mechanism.

4.5. **Visualization, Commissioning and Debugging Tools**

4.5.1. The product shall have an embedded web server to allow for remote data visualization.

4.5.2. The product shall have remote Single Line Diagram capabilities (accessible via a web browser).

4.5.3. The product shall have a commissioning tool that allows the user to force points and issue control commands.

- 4.5.4. The product software toolset shall include a protocol analyzer to facilitate commissioning activities.
- 4.5.5. The product software toolset shall include a system log viewer for auditing trail.
- 4.5.6. The product software toolset shall include a system statistic viewer for health monitoring.
- 4.5.7. The product software toolset shall include an IED communication dashboard to allow the user to easily monitor the substation network status.

4.6. Alarm and event management

- 4.6.1. The product shall include an alarm management system with acknowledgement/clear mechanism.
- 4.6.2. The alarm management system shall be accessible locally (via video port) and remotely (via web browser).
- 4.6.3. Any point (digital or analog) of the system shall be configurable as an alarm.
- 4.6.4. The alarm management system shall keep the alarm history in non-volatile memory.
- 4.6.5. The alarm management system shall allow the user to block/unblock alarms during normal operation.
- 4.6.6. The product shall include a Sequence of Event system that allows recording any transitions into non-volatile memory.

4.7. Passthrough

- 4.7.1. The product shall allow remote connection of native vendor tools to IED via a passthrough connection.
- 4.7.2. The passthrough connections shall be secured using TLS 1.2 or better.
- 4.7.3. The passthrough access shall be logged.
- 4.7.4. The passthrough access shall be monitored and remotely controllable.
- 4.7.5. The user activities of a passthrough sessions shall be recorded, using a complementary product.

4.8. Logic capabilities

- 4.8.1. The product shall include an embedded logic module allowing to create logical points and to perform the following operations :
 - Analog control from analog input value
 - Binary control from binary input state
 - Best of function (on analog and binary inputs)
 - Binary debouncing
 - Force point value from control operation (on analog and binary inputs)
 - Grouped Control
 - Inhibition management from control operation
 - Input latch and reset
 - Logical (AND, OR, NOT, etc)
 - Arithmetic (add, subtract, multiply, etc)
 - Relational (less than, greater than, etc)
 - Conditions (if Then Else, etc)
 - Math (Abs, Exp, Log, Sin, Cos, Min, Max, etc)

- Statistics (average)

4.8.2. The trigger for the evaluation of each equation shall be user configurable :

- On a periodic basis
- By exception on any value change
- By exception on a selectable value change

4.8.3. The product shall also support IEC 61131-3 compatible Soft PLC engine supporting the following programming languages :

- Instruction List
- Structured Text
- Functional Block Diagram
- Continuous Function Chart
- Ladder Diagram
- Sequential Functional Chart

4.8.4. The Soft PLC engine shall offer a complete programming environment with full debugging support (step by step, break points, etc).

4.8.5. The Soft PLC script shall be embedded in the substation gateway configuration file in order to make configuration file management easier.

4.8.6. Soft PLC scripts shall be easily reusable. Scripts' variable shall not be directly tied to the substation gateway tags.

4.9. Time synchronization

4.9.1. The product shall have a RTC (real time clock) that maintain a good accuracy in free-running mode (when disconnected from the time source) or when the unit is powered off.

4.9.2. The product's RTC shall be synchronize using one or many of the following sources :

- IEEE Std 1588™-2008 standard (PTP – Precision Time Protocol)
- Demodulated IRIG-B
- Modulated IRIG-B
- SNTP
- SCADA protocols that supports “set time” command, such as DNP3.
- Manual operation

4.9.3. The product's shall be able to synchronize IEDs using one or many of the following method :

- IEEE Std 1588™-2008 standard (PTP – Precision Time Protocol)
- Demodulated IRIG-B (dedicated output or via serial ports – jumperless configuration)
- SNTP
- Protocols that supports “set time” command, such as DNP3.

4.9.4. High precision demodulated IRIG-B distribution shall allow for phasor measurement unit (PMU) synchronization. (assuming demodulated IRIG-B input is provided)

4.9.5. When multiple time sources are available, the product shall automatically select the best time source available based on time quality of each source.

4.9.6. The user shall be able to configure the time precision criteria for which the product should be considered to be synchronized.

4.9.7. The product shall support automatic time zone adjustment.

4.9.8. All time events (updates, source change, etc.) shall be logged.

4.10. **Robustness**

4.10.1. The product shall have a robust Ethernet implementation. Such robustness shall be confirmed by a third party test certification such as Wurltech Achilles communication certification.

4.10.2. The product shall pass the NESSUS vulnerability scan and results shall be available.

4.11. **Certifications and compliance**

4.11.1. The product shall have a KEMA certificate for its IEC 61850 client implementation.

4.11.2. The product's DNP3 implementation shall comply with level 2 compliance tests. The compliance shall be listed on the www.dnp.org website.

5. **Licensing and upgrades**

5.1. The licensing model shall be flexible and scalable.

5.2. The product shall be remotely upgradable.

5.3. Product upgrades shall be made available free of charge.

5.4. New software options/modules shall also be made available for installed products, when feasible. Additional fees may apply.

6. **Operating System**

6.1. The product shall be based on an embedded operating system.