1. **Scope**

This specification describes the features and specifications of the SMP IO-2330-S, as part of Eaton’s substation automation solution. The SMP IO-2330-S is designed to work as a standalone product or with a complementary product such as an SMP Gateway automation platform, IED Manager Suite (IMS) and Visual T&D.

1. **Applicable Standards**

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

1. **Hardware Features**
	1. **Form factor**
		1. The product shall be available in 19’’ rack mount with 3U.
	2. **Power supply**
		1. The product shall have a power supply to operate at low voltage, 24/48 VDC.
	3. **Front Panel**
		1. The product shall have an individual LED for each input and output.
		2. The product shall have a test button for LED Test.
		3. The product shall have a Local/Remote button to enable/disable remote command.
	4. **Communication interfaces**
		1. The product shall have at least one independent Ethernet port, with an internal switch and two Ethernet connectors, to be used for daisy chaining multiple IO-2330-S units’ connectivity.
		2. The product shall have options for metallic and optical Ethernet (LC connectors).
		3. The product shall have a USB port on the front panel for maintenance purposes.
	5. **Time synchronization**
		1. The product shall have demodulated IRIG-B input.
	6. **Physical inputs/outputs**
		1. The product shall support 64 status input with 24,48,125 VDC voltage range options.
		2. The product shall have at least 2 built-in Form C output relays.
	7. **Type tests and certifications**
		1. The product shall have cTUVus Marking.
		2. The product shall be RoHS compliant.
		3. The product shall be WEEE compliant.
		4. The product shall be REACH compliant.
		5. The product shall have an operating temperature of -40° to 85° Celsius (-40° to 185° Fahrenheit).
2. **Software features**
	1. **Protocols and data concentration**
		1. The product shall support most industry-standard protocols for gathering data from IEDs:
* IEC 61850-8-1 GOOSE
	+ 1. The product shall support most industry-standard protocols for sending data to control centers or enterprise applications:
* DNP3 (IEEE Std 1815™-2012 standard)
* IEC 61850-8-1 MMS
* IEC 61850-8-1 GOOSE
	1. **Security**
		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 allow 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.
		1. All product firmware components shall be digitally signed by the manufacturer. Such signatures shall be verified by the device on firmware installation/upgrade and on device start-up.
		2. The product shall tie into enterprise level software allowing for:
* Central user account management
* IED configuration management
* IED event processing
* IED password management
* IED update management
	+ 1. 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.
		2. 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.
		3. The product shall implement secure SCADA protocols as defined by IEC 62351-5. This shall include DNP3 Secure Authentication.
		4. The product shall support X.509 certificates for authentication.
		5. The product shall have a built-in firewall.
	1. **Configuration tools**
		1. The configuration tool shall allow off-line configuration of the product.
		2. The configuration tool shall be template driven.
		3. The configuration tool shall have import/export capabilities in an Excel-compatible format.
		4. The configuration tool shall support copy/paste from/to an Excel spreadsheet.
		5. The configuration tool shall have import/export capabilities for IEC 61850 server protocols (.icd files).
		6. The configuration tool shall have import/export capabilities for IEEE Std 1815™-2012 standard (DNP3) server protocols (DNP XML Device Profile format).
		7. The configuration toolset shall support versioning.
		8. The configuration toolset shall be backward compatible – it shall allow the configuration of older firmware versions and conversion to newer version.
		9. The configuration tool shall include a configuration parameter validation mechanism.
	2. **Visualization, commissioning and debugging Tools**
		1. The product shall have an embedded web server to allow for remote data visualization.
		2. The product shall have a commissioning tool that allows the user to force points and issue control commands.
		3. The product software toolset shall include a protocol analyzer to facilitate commissioning activities.
		4. The product software toolset shall include a system log viewer for auditing trail.
		5. The product software toolset shall include a system statistic viewer for health monitoring.
	3. **Logic capabilities**
		1. The product shall also support IEC 61131-3 compatible SoftPLC engine supporting the following programming languages:
			+ - Instruction List
				- Structured Text
				- Functional Block Diagram
				- Continuous Function Chart
				- Ladder Diagram
				- Sequential Functional Chart
		2. The SoftPLC engine shall offer a complete integrated development environment (IDE).
		3. The SoftPLC script shall be embedded in the configuration file in order to make configuration file management easier.
		4. SoftPLC scripts shall be easily reusable. Script variables shall not be directly tied to the internal database tags.
	4. **Time synchronization**
		1. The product shall have an RTC (real time clock) that maintains enough accuracy when disconnected from the time source or when the unit is powered off.
		2. The product’s RTC shall be synchronize using one or many of the following sources:
			+ - Demodulated IRIG-B
				- SNTP
				- SCADA protocols that supports “set time” command, such as DNP3.
				- Manual operation
		3. When multiple time sources are available, the product shall automatically select the best time source available based on time quality of each source.
		4. The product shall support automatic time zone adjustment.
		5. All time events (updates, source change, etc.) shall be logged.
	5. **Robustness**
		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.
		2. The product shall pass the NESSUS vulnerability scan and results shall be made available on request.
	6. **Certifications and compliance**
		1. The product’s DNP3 implementation shall comply with level 2 compliance tests.
1. **Licensing and upgrades**
	1. The licensing model shall be flexible and scalable.
	2. The product shall be remotely upgradable.
	3. Product upgrades shall be made available free of charge.
	4. New software options/modules shall also be made available for installed products, when feasible. Additional fees may apply.
2. **Operating system**
	1. The product shall be based on an embedded Linux operating system.