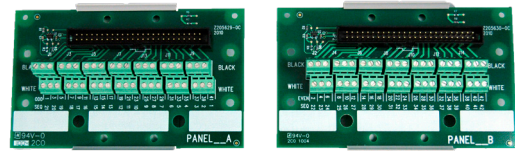


BCPM Series Panelboard Monitoring Systems

BCPMSCE

User Guide

Panelboard Monitoring System with Ethernet Communication,
Split-Core Branch Current Sensors
Z206857-0C
04/2020



Safety Information

Important information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service or maintain it. The following special messages may appear throughout this bulletin or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of either symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.



CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

Notice is used to address practices not related to physical injury.

Safety Precautions

  **DANGER**

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 in Canada, or applicable local codes.
- Read and understand the instructions before installing the product. Follow the instructions during installation.
- Installation, wiring, testing or service must be performed only by qualified persons in accordance with all applicable codes and regulations.
- Install the product in an appropriate electrical and fire enclosure per local regulations.
- Do not use the product for life or safety applications.
- Do not install the product in hazardous or classified locations.
- Do not exceed the product's ratings or maximum limits.
- The product may use multiple voltage/power sources.
- Turn off ALL power supplying equipment before working on or inside the equipment.
- Use a properly rated voltage sensing device to confirm that all power is off.
- Do NOT depend on the product for voltage indication.
- Products rated only for basic insulation must be installed on insulated conductors.
- Current transformer secondaries (current mode) must be shorted or connected to a burden at all times.
- Remove all wire scraps and tools, replace all doors, covers and protective devices before powering the equipment.

Failure to follow these instructions will result in death or serious injury.

A qualified person is one who has skills and knowledge related to the construction and operation of this electrical equipment and installations, and has received safety training to recognize and avoid the hazards involved. NEC Article 100

If this product is used in a manner not specified by the manufacturer, the protection provided by the product may be impaired. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

Control system design must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and over-travel stop.

⚠ WARNING

LOSS OF CONTROL

- Assure that the system will reach a safe state during and after a control path failure.
- Separate or redundant control paths must be provided for critical control functions.
- Test the effect of transmission delays or failures of communication links.¹
- Each implementation of equipment using communication links must be individually and thoroughly tested for proper operation before placing it in service.

Failure to follow these instructions may cause injury, death or equipment damage.

¹For additional information about anticipated transmission delays or failures of the link, refer to NEMA ICS 1.1 (latest edition). Safety Guidelines for the Application, Installation, and Maintenance of Solid-State Controls or its equivalent in your specific country, language, and/or location.

Provide a disconnect device to disconnect the meter from the supply source. Place this device in close proximity to the equipment and within easy reach of the operator, and mark it as the disconnecting device. The disconnecting device shall meet the relevant requirements of IEC 60947-1 and IEC 60947-3 and shall be suitable for the application. In the US and Canada, disconnecting fuse holders can be used. Provide overcurrent protection and disconnecting device for supply conductors with approved current limiting devices suitable for protecting the wiring.

For use in a Pollution Degree 2 or better environment only. A Pollution Degree 2 environment must control conductive pollution and the possibility of condensation or high humidity. Consider the enclosure, the correct use of ventilation, thermal properties of the equipment, and the relationship with the environment.

FCC Notice

FCC PART 15 INFORMATION

NOTE: This equipment has been tested by the manufacturer and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Modifications to this product without the express authorization of the manufacturer nullify this statement.

This Class A digital apparatus complies with Canadian ICES-003.

Specifications

Table 1: Specifications

Type	Description
Voltage Inputs	
Measurement Voltage	90 to 300 Vac line-to-neutral, 50/60 Hz
Control Power	100 to 277 Vac line-to-neutral, 50/60 Hz, 15 VA max.
Frequency	50/60 Hz
Accuracy	
Power/Energy	IEC 62053-21 Class 1, ANSI C12.1-2008 (1% system accuracy includes both the BCPMSCE main unit and 50 A or 100 A branch current sensors)
Voltage	±0.5% of reading 90 to 277 V line-to-neutral
Current	±0.5% of reading
Minimum ON Current	50 mA
Operation	
Sampling Frequency	2560 Hz
Update Rate	Modbus: 1.8 seconds (both panels) BACnet: 14 seconds SNMP: 20 seconds
Ethernet Communication	
Physical Interface	RJ45 connector with 10/100 Mbit Ethernet
Protocols Supported	Modbus TCP, BACnet IP, SNMP V2c
Serial Communication	
Physical Interface	2-wire RS-485
Serial Protocols Supported	Modbus RTU or BACnet MS/TP
Address Range	1 to 247 for Modbus RTU; 0 to 127 for BACnet MS/TP
Baud Rate	9600, 19200, 38400
Parity	Modbus RTU: NONE, ODD, EVEN BACnet MS/TP: NONE (fixed)
Communication Format	8 data bits, 1 start bit, 1 stop bit
Termination	2x3 position connector
Wire Size	Up to 16 AWG
Wire Size Range	
Aux CT Terminals	24 to 14 AWG
Voltage Input and Control Power Connectors	22 to 12 AWG
Terminals on CT Adapter Boards	26 to 16 AWG
Terminal Block Torque	
Aux CT Terminals	3.5 to 4.4 in-lb (0.4 to 0.5 N-m)
Voltage Input and Control Power Connectors	4.4 to 5.3 in-lb (0.5 to 0.6 N-m)
Terminals on Branch CT Adapter Boards	1.9 to 2.2 in-lb (0.22 to 0.26 N-m)
Mechanical	
Ribbon Cable Support	4 ft. (1.2 m) flat ribbon cable ships standard; up to 20 ft. (6 m) flat or round ribbon cables are available
Environmental	
Operating Temperature Range	0 to 60 °C (32 to 122 °F) (<95% RH, non-condensing)
Storage Temperature Range	-40 to 70 °C (-40 to 158 °F)
Altitude of Operation	3000 m

Type	Description
Compliance Information	
Agency Approvals	UL508 open type device**, IEC/EN61010-1
Installation Category*	Cat. III, Pollution Degree 2
Conducted and Radiated Emissions	FCC part 15 Class A, EN55011/EN61000-6-4 Class A (heavy industrial)
Conducted and Radiated Immunity	EN 61000-6-2 and EN 61326-1

*For indoor use only.

**BCPM internal circuitry (cables and CTs) are not circuits as defined by UL508A, as they do not extend beyond the BCPM itself without further safety/fire isolation.



Note: The CE mark indicates RoHS2 compliance. Please refer to the CE Declaration of Conformity for additional details.

Introduction

The PowerLogic™ BCPMSCE Series panelboard monitoring system is designed to measure the current, voltage, and energy consumption of up to 92 circuits (84 branch circuits, two 3-phase mains, two neutrals), enabling users to monitor two panelboards or an entire data center PDU with a single product. It also includes Ethernet capability, allowing communication in multiple protocols.

The BCPMSCE consists of a data acquisition module, up to 4 current sensor adapter boards and up to 84 split-core current sensors (50 A, 100 A, or 200 A), with eight auxiliary inputs. Each conductor passes through the appropriate current sensor before terminating at the breaker. Each sensor transmits the current data to the data acquisition board. The BCPMSCE measures both current and power for the mains and branch circuits. The BCPMSCE can easily accommodate different panel configurations, including any combination of multi-phase breaker positions, voltage phase mapping, and breaker sizes. To configure the BCPMSCE for operation, use the Schneider Electric ION Setup configuration software tool. Get the latest version at <https://schneider-electric.box.com/ionsetuplatest>.

Data is transmitted via Ethernet with Modbus TCP, BACnet IP or SNMP protocol, or via RS-485 with Modbus RTU or BACnet MS/TP protocols. Some protocols can be used simultaneously, and the Ethernet protocols all support access by multiple masters. Each data acquisition board requires two Modbus addresses, one for each set of 42 current sensors, and four auxiliary inputs. When a circuit exceeds the user-defined thresholds, the BCPMSCE activates the event indicators. The communication interfaces and protocols require some configuration at the time of installation.

Figure 1 Branch Circuit Power Meter with Ethernet Communication



Parts of the BCPMSCE

Figure 2 shows the parts of the BCPMSCE, while Table 2 describes these parts.

Figure 2 BCPMSCE Panel Board Monitoring System

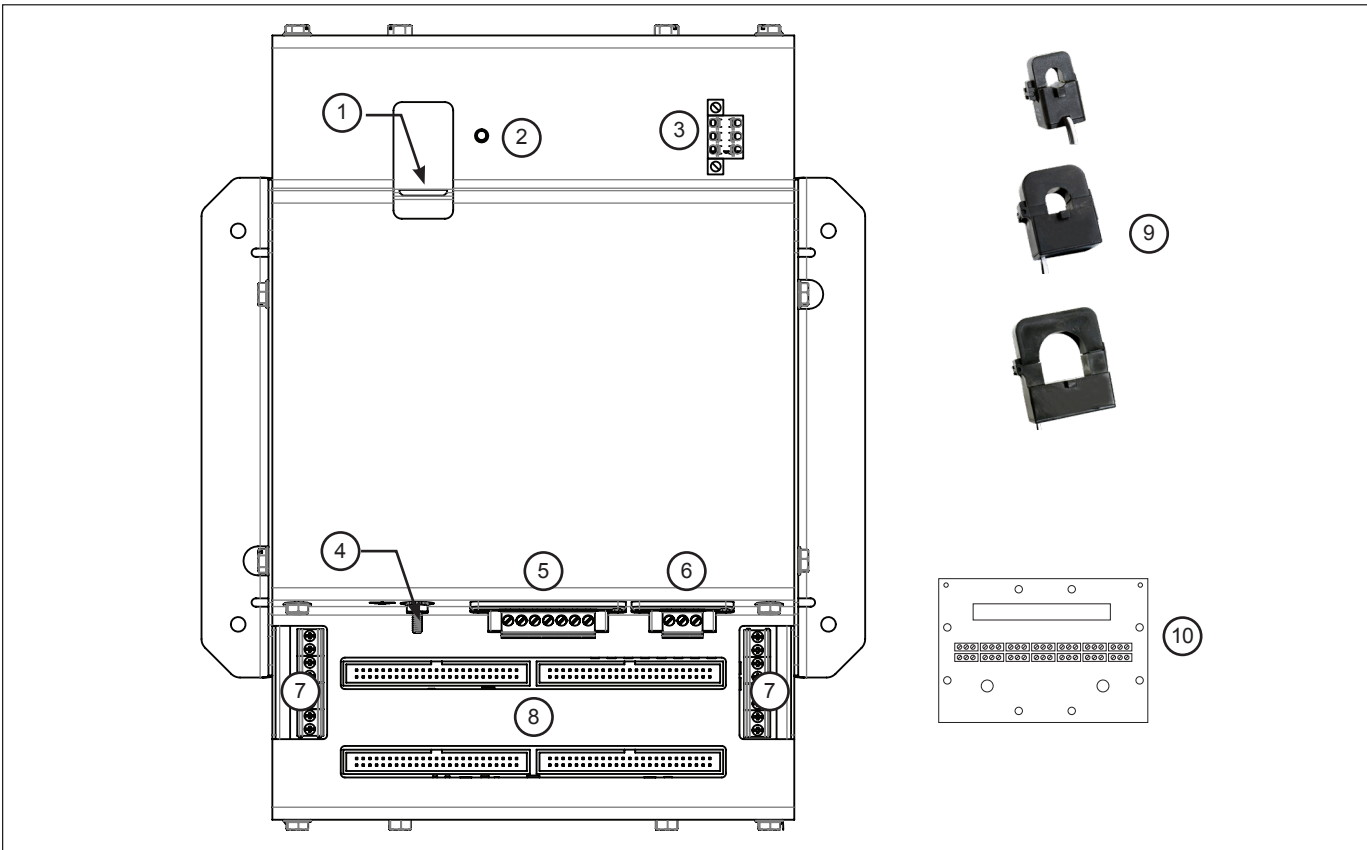


Table 2: Parts Description of the BCPMSCE

Part	Description
1 Ethernet port	Provides Ethernet connection for the gateway component.
2 Power LED	Indicates power is applied to the meter.
3 2x3 RS-485 serial connection	Used for Modbus, BACnet, and SNMP serial communications.
4 Protective ground connection	Provides a grounding point for the device.
5 Voltage taps	1, 2, or 3 phase plus neutral connections. For voltage sensing and power calculations.
6 Control power connection	Provides power to operate the meter.
7 Auxiliary CT inputs	These 0.333 Vac inputs are used for monitoring the main breaker or other high amperage source. Inputs on the left are for panelboard 2; inputs on the right are for panelboard 1.
8 50-pin ribbon cable connectors	48-inch (1220 mm) ribbon cables are provided for easy connection of the adapter boards to this point of the data acquisition board. Other ribbon cable lengths are available (sold separately). The two connectors on the left are for panelboard 2; the two on the right are for panelboard 1. Connect adapter boards A and B to the correct ribbon cable connectors for each panel. The top connectors are for Board B, and the bottom connectors are for Board A.
9 Current sensors	Up to 84 sensors can be used with the BCPMSCE.
10 Adapter board	Includes connectors for a ribbon cable and up to 42 current sensors.

Dimensions

Figure 3 Housing and Mounting Brackets

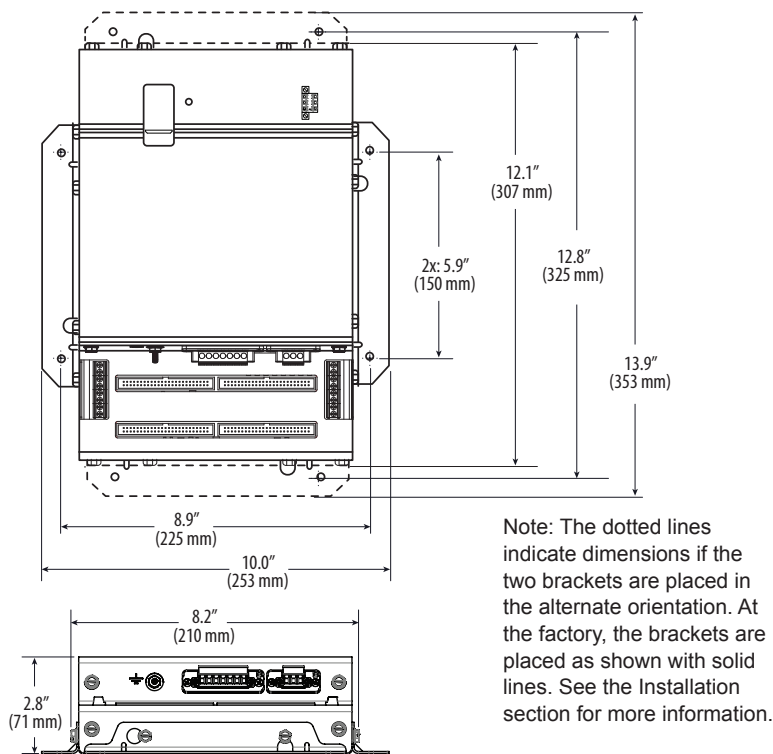
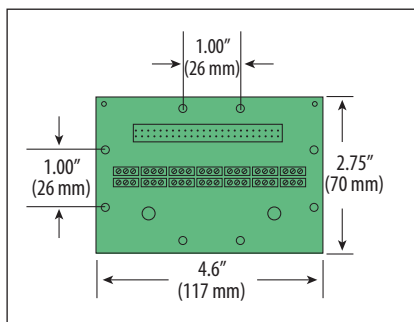
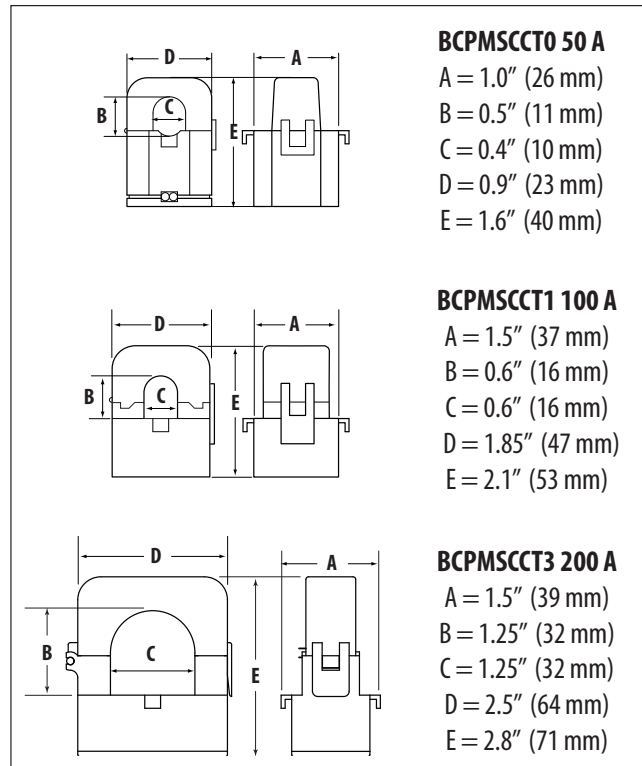


Figure 4 Adapter Board and Current Sensors





Data Output

The BCPMSCE provides several types of measurements that give a comprehensive view of power consumption for every monitored load on the panel:

- Real-time measurements: A live and up-to-date view of present power levels and the factors that affect them.
- Demand measurements: Averages of values measured over a specified time interval. The time interval (typically 15 minutes) can be set from 10 seconds to more than a day. The demand calculation can be configured to use single intervals or the sliding average of up to 6 sub-intervals. Demand measurements are useful for tracking or graphing load levels over time to correlate with total energy consumption.
- Historic maximum measurements: These measurements store the largest value recorded for a specific measurement since the last time they were cleared. They are useful for identifying peak levels critical to equipment sizing or demand limits in utility agreements.
- Accumulated energy measurements: Ongoing totals of cumulative energy used since the last time the value was cleared. Energy values provide the informational basis for billing, cost allocation, carbon offset, BTU equivalent calculations, and other applications of overall energy use.
- Energy snapshots: Energy totals that only change when the demand intervals are updated. They are samples of the free-running energy accumulators at the end of each demand interval, as configured by the user. These provide energy readings that are easily correlated to the demand values to simplify the tasks of sub-billing and cost allocation.
- Over-threshold Events (previously referred to as Alarms): Provide a warning of excessively high or low current on each branch and aux channel. The user can set two high-level and two low-level thresholds, and a delay time for latching events. Events are reported as both non-latched events and latched events. Non-latching events are active while the current exceeds the threshold, but go inactive if the current

returns to a level within the specific thresholds. Latching events become active when the current exceeds the threshold for a time period greater than the specified delay and remain active until they are cleared remotely. Event status can be polled via any protocol. Via BACnet, Subscribe_COV can be used to generate event notifications. Via SNMP, they drive SNMP event notifications.

Advanced Features - The BCPMSCE supports a number of advanced features. Some are always active, and others are configured manually via Modbus register 62017, BACnet object AV164, or SNMP MIB variable "spanels/panel1/p1Configuration/p1Setup/p1UserDefinedSettings" (OID .1.3.6.1.4.1.3833.1.30.1.1.6.3.4.0). For models with 42 channels or more, these features are configured independently for each panel.

- Logical meter support: The BCPMSCE can be configured to map any set of 1, 2 or 3 channels that are adjacent in the panel to a logical meter, referred to in the point map as a logical circuit, that provides accurate multi-phase measurement totals. Map these logical circuits by writing the desired logical circuit number into a set of registers/data objects provided for each branch and aux channel (per panel).
- The channels assigned to each logical circuit must be adjacent in the panel (usually used for multi-phase breakers), but there are no limitations on where those adjacent channels are aligned in the panel (any position where a multi-phase breaker can be installed). This functionality is always active, but a user selection affects the how the data can be accessed via Modbus. Measurement data via Modbus for logical circuits is presented in two ways, arranged either by logical circuit number (looks more like a collection of individual meters) or by measurement type (arranged similar to the single-phase data section of the point map).
- Legacy point map or alternate logical circuit point map: The BCPMSCE can be configured to select a preferred version of the Modbus registers in the address range 4000 to 9999. If enabled (default), the logical circuits by measurement type is active. Otherwise, the legacy point maps for 2-phase and 3-phase breakers used in BCPMSCE models with a firmware version earlier than 1.023 is active. The logical circuits functionality can also be accessed via the "Logical Circuits by Circuit" section of the point map (address range 10000 to 45000), regardless of the state of this selection.
- Phase angle measurements: The BCPMSCE measures the phase angle of every voltage and current input and presents these measurements (in degrees) in additional data registers/objects. These values are used to verify that current inputs are assigned to the proper voltage phases and to help determine how power factor variations are influenced by current phase changes vs. harmonic distortion. Phase angle measurements are instantaneous and always active.
- User CT phase assignment: In the default mode, the BCPMSCE assigns each channel to the corresponding phase that most 3-phase panels implement, so that the user does not have worry about it. The user can opt to replace this self-assignment paradigm with a mode that allows explicit specification of the phase assignment for each channel. The explicit assignments set by the user are stored by the BCPMSCE in non-volatile memory.
- Phase angle reference: The BCPMSCE measures the phase angle of every current and voltage input. The user can select whether the phase angles are stated relative to an absolute reference (the phase angle of voltage input V1) or relative to the voltage phase assigned to that specific current input channel.
- Signed power: Users can configure the BCPMSCE to report power as a signed value indicating whether the power is currently being delivered (imported from the grid) or received (exported to the grid) for channels with generation sources or bi-directional (regenerative)

loads. When signed power is disabled, the energy accumulators include all energy measured, regardless of direction. When signed power is enabled, the energy accumulators only include all energy delivered (imported from the grid).

- Signed power factor: By default the BCPMSCE reports power factor as an unsigned value. The user can set it to report as a signed value, where the sign indicates whether the current phase angle leads or lags the corresponding voltage phase.
- Demand/snapshot time interval source: The BCPMSCE offers two mechanisms for driving the demand/snapshot time interval, an interval timer or an RTC (real-time clock). The legacy mode (default) uses an interval timer that does not need to be set to an absolute time. When using the interval timer the demand/snapshot interval can be set from 10 to 32767 seconds (over 9 hours). An alternate mode utilizes an RTC set to a specific date and time to synchronize the results with a larger system. The RTC must first be set in order to run and capture demand values and energy snapshots. When power is interrupted, the RTC resets to a default date and time and must be set again in order to run. When using the RTC, the demand/snapshot interval can be set from 10 to 3600 seconds (1 hour).

Table 3: Data Outputs Table

Monitoring of Mains	
Real Time Measurements	Current: multi-phase average and per phase
	Current phase angle
	Real power (kW): multi-phase total and per phase
	Apparent power (kVA): multi-phase total and per phase
	Power factor: multi-phase average and per phase
	Voltage - L-L: multi-phase average and per phase
	Voltage - L-N: multi-phase average and per phase
	Frequency (phase A)
Demand Measurements	Current present demand: multi-phase average and per phase
	Real Power (kW) present demand: multi-phase average and per phase
Historic Maximums	Maximum instantaneous current: multi-phase average and per phase
	Maximum current demand: multi-phase average and per phase
	Maximum real power demand: multi-phase total and per phase
Accumulated Energy	Energy (kWh): multi-phase total and per phase
Energy Snapshots	Energy (kWh): multi-phase total and per phase
Monitoring of Branch Circuits	
Real Time Measurements	Current: multi-phase average and per phase
	Current phase angle per branch
	Real power (kW): multi-phase total and per phase
	Apparent power (kVA): multi-phase total and per phase
	Power factor: multi-phase average and per phase
Demand Measurements	Current present demand: multi-phase average and per phase
	Real power (kW) present demand: multi-phase average and per phase
Historic Maximums	Maximum instantaneous current: multi-phase average and per phase
	Maximum current demand: multi-phase average and per phase
	Maximum real power demand: multi-phase total and per phase
Accumulated Energy	Energy (kWh): multi-phase total and per phase
Energy Snapshots	Energy (kWh): multi-phase total and per phase
Modbus Events	
Events	Voltage over/under
	Branch current over/under
	Mains current over/under


Split Core Current Sensors

Table 4: Current Sensor Specs

	50 A	100 A	200 A
Voltage Rating	300 Vac	300 Vac (CE), 600 Vac (UL)	300 Vac (CE), 600 Vac (UL)
Measurement Range	60 A*	120 A*	240 A*
Temperature	0 to 60 °C (32 to 122 °F)	0 to 60 °C (32 to 122 °F)	0 to 60 °C (32 to 122 °F)
Agency	UL61010 Recognized, EN61010-1	UL61010 Recognized, EN61010-1	UL61010 Recognized, EN61010-1

*Momentary.

Installation


DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 in Canada, or applicable local codes.
- Read and understand the instructions before installing the product. Follow the instructions during installation.
- Installation, wiring, testing or service must be performed only by qualified persons in accordance with all applicable codes and regulations.
- Install the product in an appropriate electrical and fire enclosure per local regulations.
- Do not use the product for life or safety applications.
- Do not install the product in hazardous or classified locations.
- Do not exceed the product's ratings or maximum limits.
- The product may use multiple voltage/power sources.
- Turn off ALL power supplying equipment before working on or inside the equipment.
- Use a properly rated voltage sensing device to confirm that all power is off.
- Do NOT depend on the product for voltage indication.
- Products rated only for basic insulation must be installed on insulated conductors.
- Current transformer secondaries (current mode) must be shorted or connected to a burden at all times.
- Remove all wire scraps and tools, replace all doors, covers and protective devices before powering the equipment.

Failure to follow these instructions will result in death or serious injury.

A qualified person is one who has skills and knowledge related to the construction and operation of this electrical equipment and installations, and has received safety training to recognize and avoid the hazards involved. NEC Article 100

If this product is used in a manner not specified by the manufacturer, the protection provided by the product may be impaired. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

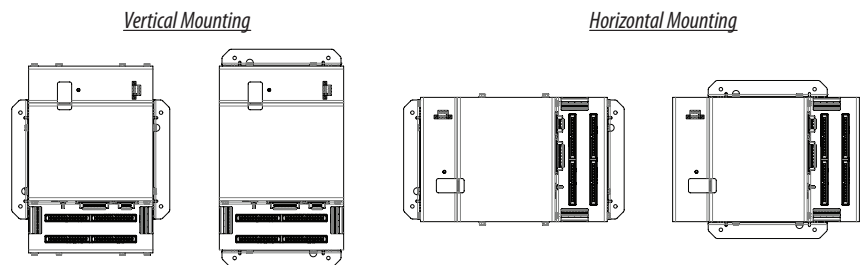


Observe precautions for handling static sensitive devices to avoid damage to the circuitry that is not covered under the factory warranty.

⚠ ⚠ The protective ground connection on the housing should be used if the device will not be mounted to a suitably grounded surface. Assure conductivity to the protective ground.

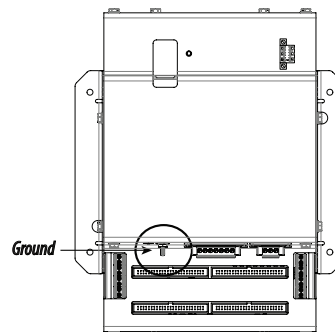
1. Determine where you will mount the BCMPMSCE measurement unit. The preferred location is inside the enclosure of the panelboard being monitored. If sufficient space is not available there, then mount the unit in an appropriate enclosure nearby. Decide whether to mount it vertically or horizontally. The meter is shipped with the brackets placed for vertical mounting. If desired, you can move the brackets from the sides to the ends of the housing. Loosen the screws on the sides of the BCMPMSCE that hold the brackets in place (do not fully remove the screws from the housing). Loosen the screws on the two ends of the housing (do not fully remove the screws from the housing), and set the brackets into their new positions. Tighten all screws to 25 in-lb (2.8 N-m).

Figure 5 Brackets positioned for vertical and horizontal mounting



2. Install the BCMPMSCE in the panel. A grounding connection is located on the housing (see below).

Figure 6 BCMPMSCE ground stud

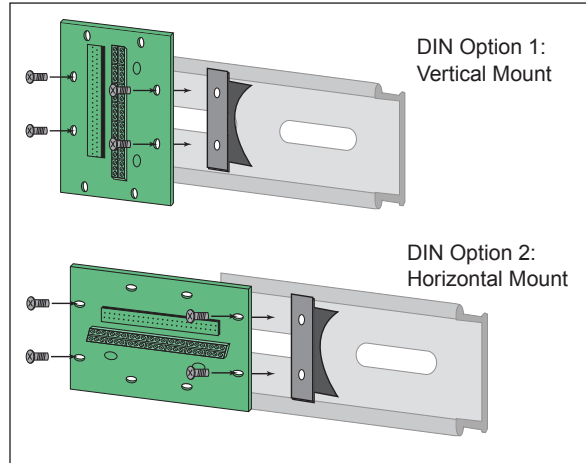


3. Choose a location to mount the adapter boards. If space permits, mount them in the panelboard being monitored. There are two channel numbering configurations available, for different applications (see the examples below). Odd/even numbering is used with panelboards that have odd numbers on one side (usually the left side) and even numbers on the other. Sequential numbering is generally used in other applications, where the panelboard has breakers numbered sequentially or where the branch circuits are used to monitor discrete loads rather than an entire panelboard. Select the configuration that best fits your application and install the adapter boards as close as you can to the location where the branch CTs will be installed. Mount the adapter boards using either DIN rail or SNAPTRACK. You can set the configuration during commissioning by writing to Modbus Register 6

(or the corresponding BACnet object or SNMP variable) or use ION Setup configuration software.

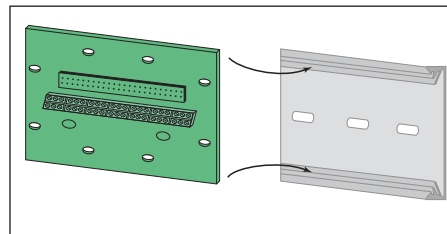
A. Use the supplied screws to secure the plastic DIN clips to the adapter board. Affix the clip to the DIN rail.

Figure 7 DIN mount configuration options



B. Secure the SNAPTRACK to the mounting surface. Click the adapter board into place.

Figure 8 SNAPTRACK mounting

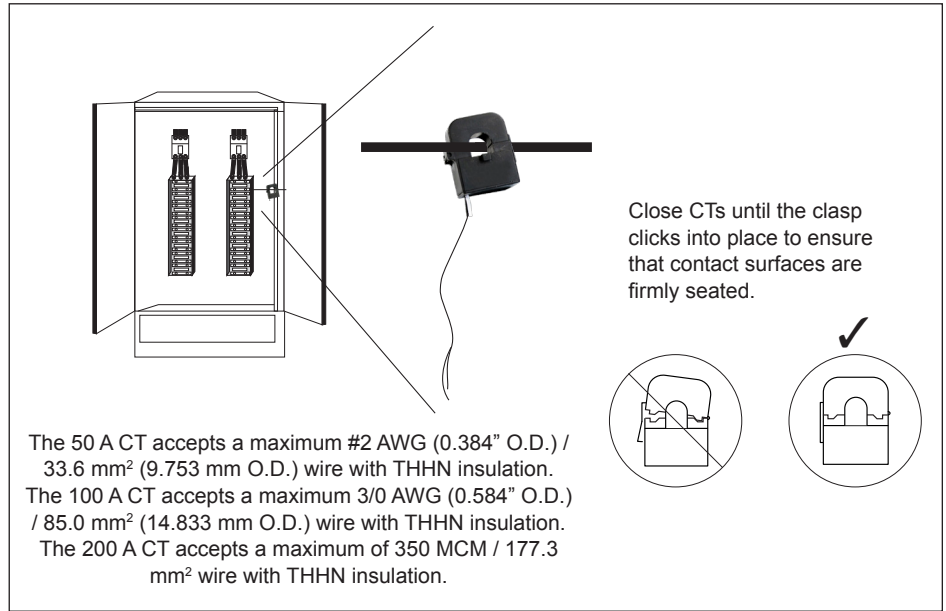


4. Install the current sensors onto the conductors to be monitored.

NOTE: If the signed power factor feature is NOT enabled, then the current sensor orientation does not affect meter behavior. If this feature IS enabled, orient the current sensors so that the arrow points toward the load for proper operation.

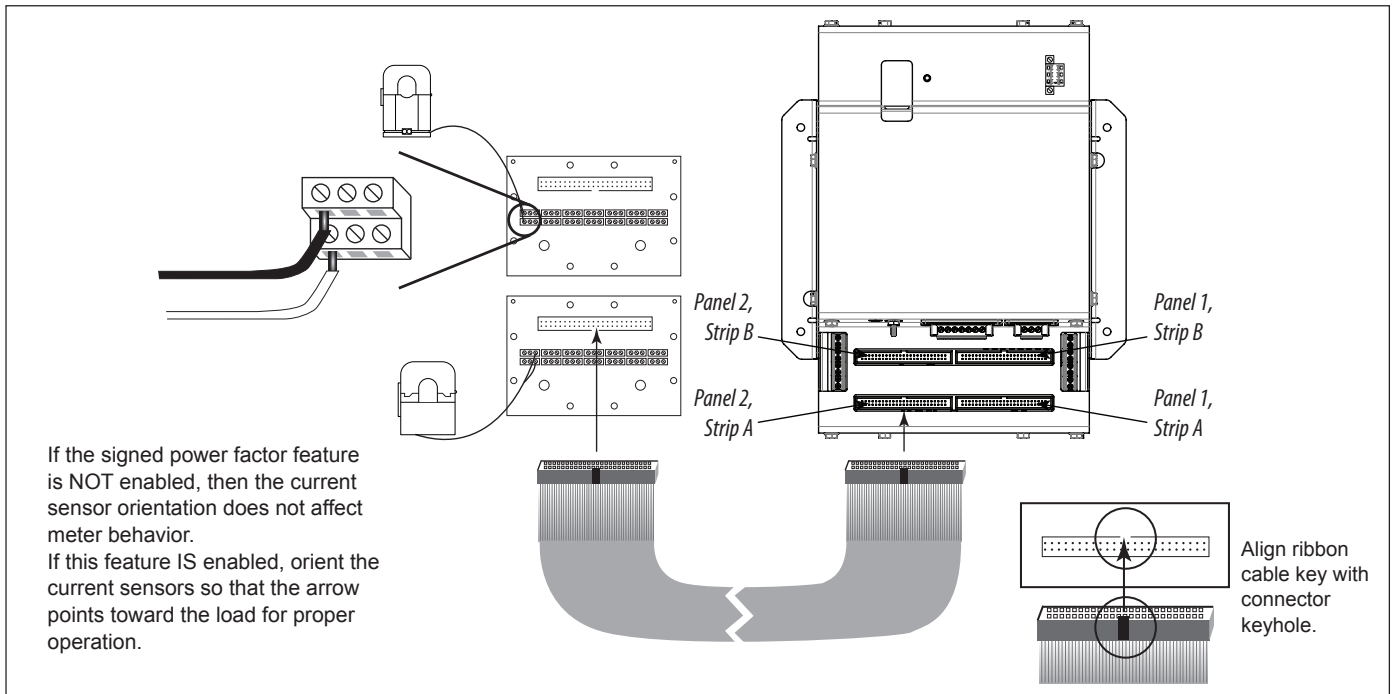
NOTE: Clean split-core contact surfaces before closing. The hinge can detach, allowing the base and the top to separate for easier cleaning and installation.

Figure 9 Install current sensors on the conductors



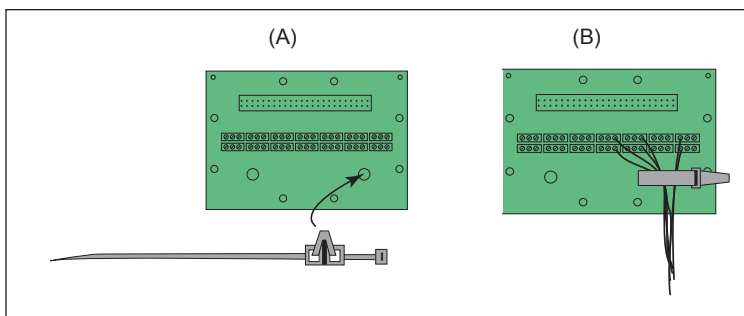
5. Connect the adapter boards to the main board using ribbon cable. Ribbon cables are keyed to ensure proper installation.
6. Connect the current sensors to the terminals on the adapter boards.

Figure 10 Connect adapter boards to main board



NOTE: Some adapter boards have serial numbers. These serial numbers are independent of the serial numbers on the main board. They do not need to match each other.

- Plastic cable ties are included with the product for strain relief. Insert the strain relief device into one of the available holes on the adapter board (A). Gather all current sensor wires connected to that adapter board and secure the cable tie around them (B).



- The adapter boards are silk screened with two rows of numbers. For applications that require odd/even branch circuit numbering, use the row designated ODD or EVEN. Odd/even numbering is used with panelboards that have odd numbers on one side (usually the left side) and even numbers on the other. For applications that require sequential numbering, use the number row marked SEQ. Sequential numbering is generally used in other applications, where the panelboard has breakers numbered sequentially or where the branch circuits are used to monitor discrete loads rather than an entire panelboard.

BLACK	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗
WHITE	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗
ODD	1	5	9	11	17	13	15	21	11	23	25	29	31	35	39	41	37	3
SEQ	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4

Adapter Board A numbering:

ODD	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41
SEQ	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

BLACK	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗
WHITE	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗
EVEN	2	6	8	12	14	18	16	20	24	26	30	32	34	36	38	40	42	40
SEQ	22	24	24	27	28	30	30	31	33	34	36	36	37	39	40	41	42	42

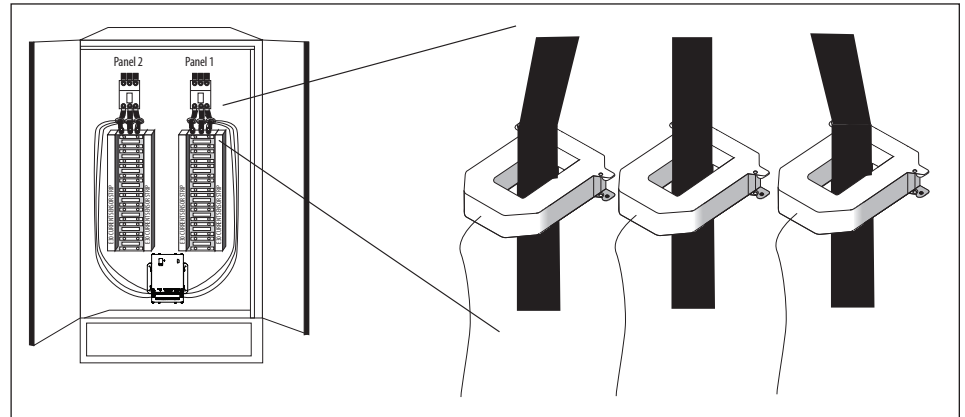
Adapter Board B numbering:

EVEN	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42
SEQ	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42

Aux CT Installation

1. Connect the (optional) 0.333 Vac current transformers (CTs) to the mains (see Figure 11), observing local codes regarding bending radius. Refer to the appropriate CT installation instructions for further information.

Figure 11 CT connection



NOTE: The BCPMSCE measures and reports the phase angle of each voltage input and each CT (when there is active current through the primary of that CT).

Wiring

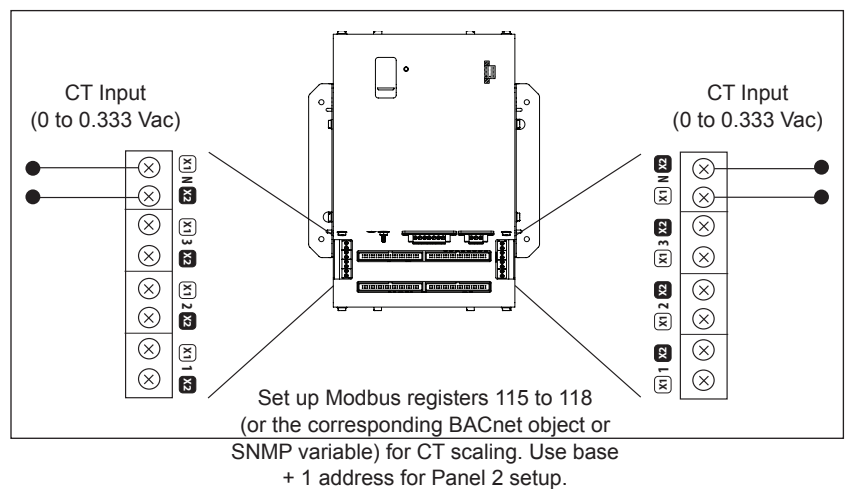
⚡ ⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- While removing or installing panels and covers, assure that they do not contact an energized bus.
- NEVER bypass external fusing.
- NEVER short the secondary of a potential transformer.
- Before closing covers and doors, carefully inspect the work area and remove any tools, wire scraps or other objects that may have been left inside the equipment.

Failure to follow these instructions will result in death or serious injury.

Figure 12 Aux CT wiring



1. Connect 2-wire 100 to 277 Vac power to the control power terminals. Observe polarity. Connect voltage lines to the voltage inputs. Provide overcurrent protection and disconnecting means to protect the wiring. Use EMFP1, EMFP2, EMFP3 fuse packs, or equivalent. Suggested: 0.5 A, time delay fuses.

Figure 13 Connect to voltage inputs

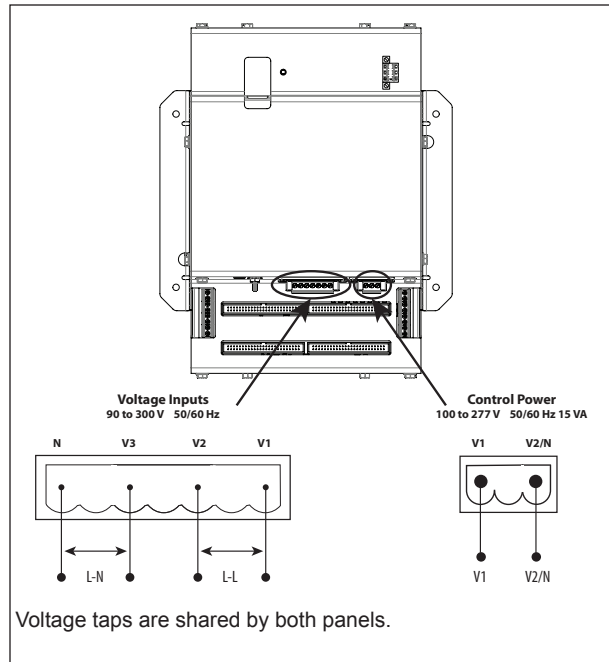
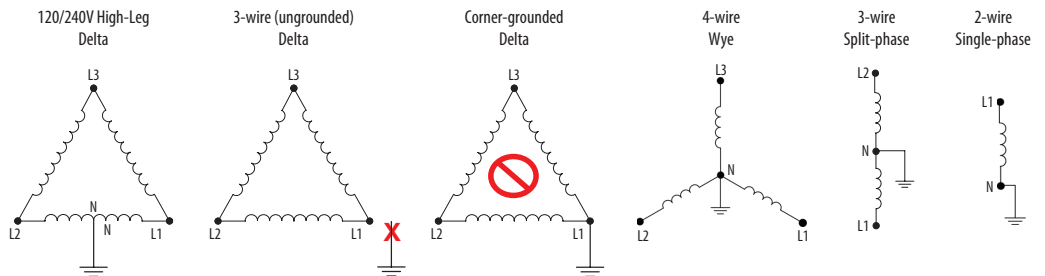


Figure 14 Wiring configurations



120 V/240 V Delta High Leg (where the center tap of one of the three phase-to-phase transformers is grounded): the BCPMSCE supports these applications, as long as the line-to neutral voltage [especially of the High Leg] does not exceed 300 Vac (as in North American 120/240 V High Leg Delta configurations).

In 3-wire (ungrounded) Delta applications, the BCPMSCE supports these applications with the following caveats:

Control Power for the meter cannot exceed 277 Vac. In applications where the L-L voltage is 277 Vac or less (e.g. 208 V line-to-line) it can be connected to two of the phases being monitored without exceeding the limit. For higher voltages (e.g. 480 V line-to-line), this must be supplied from a source that is 277 Vac or less. It could be a separate source or a transformer can be used to step it down from two of the phases being measured.

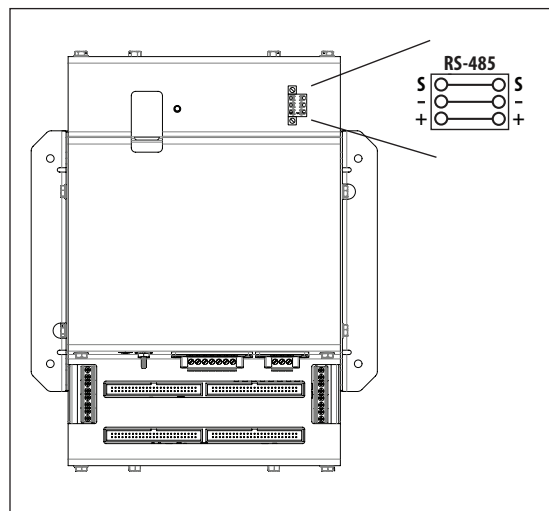
All of the CT inputs (both branches and Aux inputs) are neutral-referenced. One side of each CT is essentially connected directly to the neutral voltage input. If this is left floating, the solid-core CT strips, split-core CT adapter boards and all CTs will float at the same potential (while the panel is energized). This does not present a risk to the equipment as long as it is within 300 V of ground, but should be considered from a safety perspective in the overall application. The BCPMSCE will provide measurements in this application with the accuracy specified, with the exception of line-to-neutral voltages, which will be calculated and reported, based on a derived virtual neutral voltage, even though they are not relevant.

Corner-grounded delta: the BCPMSCE does not support these applications at any voltage level.

The BCPMSCE supports measurement of all 4-wire Wye, 3-wire split-phase and 2-wire single phase and configurations that operate between 90 and 300 Vac line-to neutral.

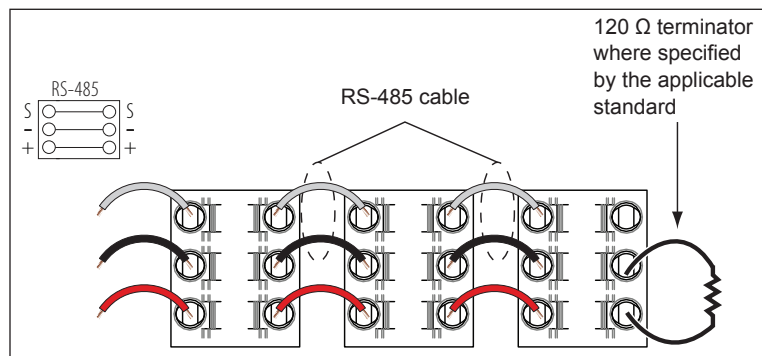
2. Connect the 2-wire Modbus RS-485 network.

Figure 15 RS-485 connection



3. Mechanically secure the RS-485 cable(s) where they enter the electrical panel.
4. If using Modbus RTU or BACnet MS/TP protocol, connect a serial cable(s) from the RS-485 loop to the serial connector on the BCPMSCE. Connect all RS-485 devices in a daisy-chain, and properly terminate the chain.

Figure 16 Daisy chain connection



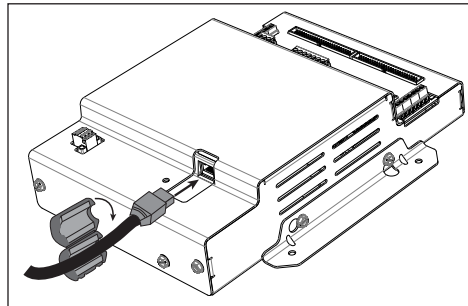
Two sets of connections are provided to simplify daisy-chain connections and enable retention of each wire.

Follow all applicable wiring and termination connection guidelines for the standard in use. Note that while both the Modbus RTU and BACnet MS/TP standards identify requirements for RS-485 line polarization/bias and termination, the value and placement of these resistors varies for each standard. The BCPMSCE does not implement any RS-485 line polarization/bias or termination internally. Shield the RS-485 cable using twisted-pair wire. Use cable that is voltage-rated for the installation. The shield is not internally connected to Earth Ground. Connect the shield to Earth Ground somewhere on the RS-485 bus (single point connection only).

5. Connect an Ethernet cable to a local PC if not already connected. Secure a ferrite filter (included) around the Ethernet cable to ensure the device meets emission requirements. Use the PC to configure the gateway (next section of this document).

Note: 100 to 277 Vac must be applied to control power inputs to supply power to the gateway during configuration.

Figure 17 Ethernet port location



6. Once configured, disconnect the local PC. If desired (and the device is configured for operation on the network), connect the BCPMSCE directly to the network for ongoing access to the GUI even if primarily using a serial protocol to access and control the BCPMSCE.

Gateway Configuration

⚠ ⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Follow safe electrical work practices. See NFPA 70E in the USA, CSA Z462 in Canada, or applicable local codes.
- Read and understand the instructions before installing the product. Follow the instructions during installation.
- Installation, wiring, testing or service must be performed only by qualified persons in accordance with all applicable codes and regulations.
- Install the product in an appropriate electrical and fire enclosure per local regulations.
- Do not use the product for life or safety applications.
- Do not install the product in hazardous or classified locations.
- Do not exceed the product's ratings or maximum limits.
- The product may use multiple voltage/power sources.
- Turn off ALL power supplying equipment before working on or inside the equipment.
- Use a properly rated voltage sensing device to confirm that all power is off.
- Do NOT depend on the product for voltage indication.
- Products rated only for basic insulation must be installed on insulated conductors.
- Current transformer secondaries (current mode) must be shorted or connected to a burden at all times.
- Remove all wire scraps and tools, replace all doors, covers and protective devices before powering the equipment.

Failure to follow these instructions will result in death or serious injury.

A qualified person is one who has skills and knowledge related to the construction and operation of this electrical equipment and installations, and has received safety training to recognize and avoid the hazards involved. NEC Article 100

If this product is used in a manner not specified by the manufacturer, the protection provided by the product may be impaired. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

Accessing the Graphical User Interface (GUI)

Note: The screen captures in this section were taken using Windows 7; other operating systems will look different.

If the BCPMSCE IP address parameters are already configured to work on the network and is being accessed from a PC on that same network, then open a web browser and enter the IP address of the BCPMSCE into the address/URL field on the browser. Press enter. On the first time login to the device GUI, follow the instructions in the section "**Accessing the GUI for the first time with firmware version 1.027 or higher**" to configure the web server's security settings and log in. If already configured, the GUI login page appears. Enter the username and password and click Login. The GUI launches and appears, as shown, in the browser window below.

Note: Devices with firmware version 1.026 and earlier will not have a login page and will not require a password.

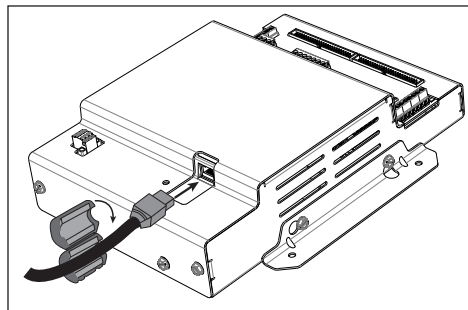
Configuration Parameters

Parameter Name	Parameter Description	Value
Operating_Mode	Operating mode: [0=Locked; 1=Discovery] Locked disables profile changes. Discovery clears profiles and auto-discovers supported devices on Restart. (Leave in Discovery mode for normal operation)	1 <input type="button" value="Submit"/>
Protocol_Mode	Primary Protocol: [1=BACnet MS/TP; 2=BACnet IP; 3=SNMP; 4=Modbus] (Modbus TCP is active in all modes) (Modbus RTU is active in modes 2 through 4) RESTART after changing to update GUI selections	4 <input type="button" value="Submit"/>
Upstream_Baud	Baud Rate of the Upstream Control serial port: (to controller - Modbus RTU or BACnet MS/TP) [9600/19200/38400/76800]	19200 <input type="button" value="Submit"/>
Modbus_Address	Default Modbus RTU Device Addresses: [1-240] The Upstream Modbus RTU addresses of the two Meter panels will be: Modbus_Address and Modbus_Address+1	1 <input type="button" value="Submit"/>
Modbus_Parity	Upstream Modbus RTU parity: [None/Even/Odd] (ignored in MS/TP mode [MS/TP is always None])	Even <input type="button" value="Submit"/>

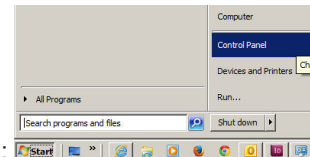
Navigation: [HELP \(?\)](#) [Network Settings](#) [System Restart](#) [Diagnostics & Debugging](#)

If the IP address parameters are not configured for the network, connect a PC directly and access the GUI from it as follows:

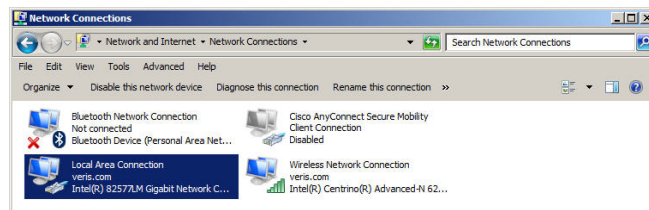
1. Connect a standard Ethernet cable between a PC and the BCPMSCE. If not already connected, secure a ferrite filter (included) around the Ethernet cable to ensure the device meets emission requirements.



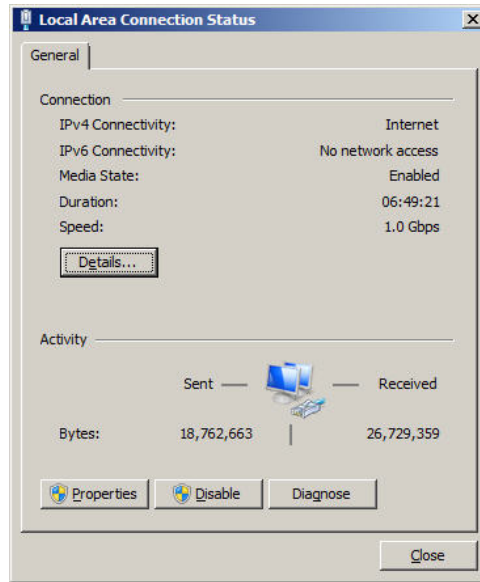
2. Temporarily change the IP address of the PC to a static value on the same subnet as the BCPMSCE. For example: If the BCPMSCE is set to its factory default IP address of 192.168.1.24, set the PC to an unused static IP address on the 192.168.1.xxx subnet (where xxx is any value between 1 and 255, except 24). Set the subnet mask to 255.255.255.0.



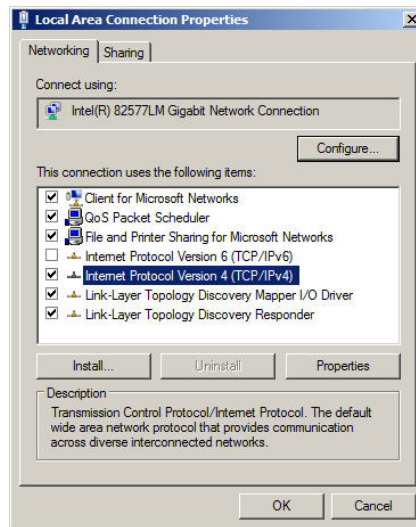
- a. Open the Control Panel:
- b. In the Control Panel, select Network and Sharing Center. In the Sharing Center, select Change Adapter Settings in the list at the upper left corner.
- c. Select the connection for the network that the BCPMSCE is connected to.



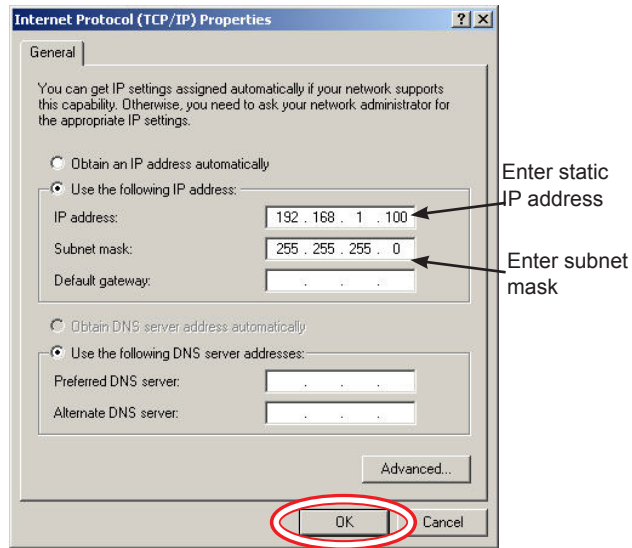
When the Local Area Connection Status dialog box appears, click on Properties.



d. Highlight Internet Protocol Version 4 (TCP/IPv4), and click OK.



e. Select <Use the following IP Address>. Make note of the IP address that appears, then enter the static IP address (e.g. if the BCPMSCE is still set to its default address of 192.168.1.24, then change it to 192.168.1.100). Enter 255.255.255.0 for the subnet mask. Click OK.

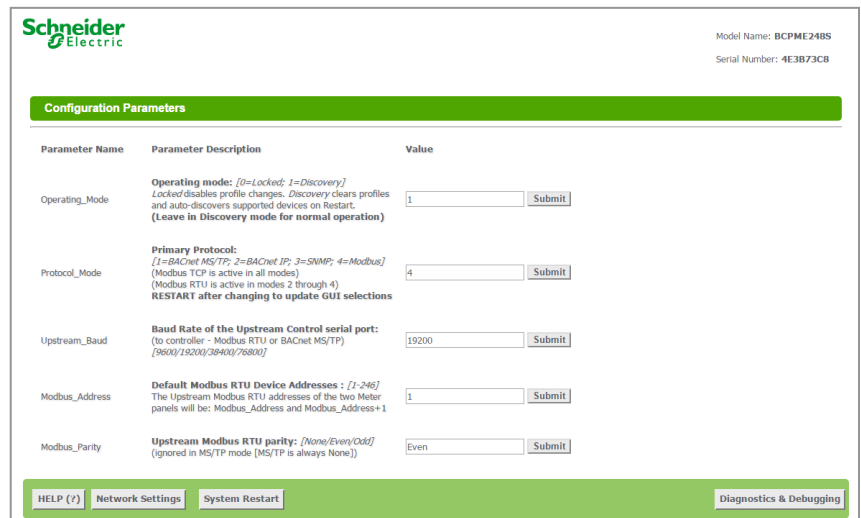


f. Click OK.

3. Open a PC web browser and enter the IP address of the BCPMSCE (default address is 192.168.1.24) to access the GUI. On the first time login to the device GUI, follow the instructions in the section "**Accessing the GUI for the first time with firmware version 1.027 or higher**" to configure the web server's security settings and log in. The GUI launches and appears in the browser window.
4. When finished using the GUI, unplug the Ethernet cable from the PC and restore the IP settings as needed.

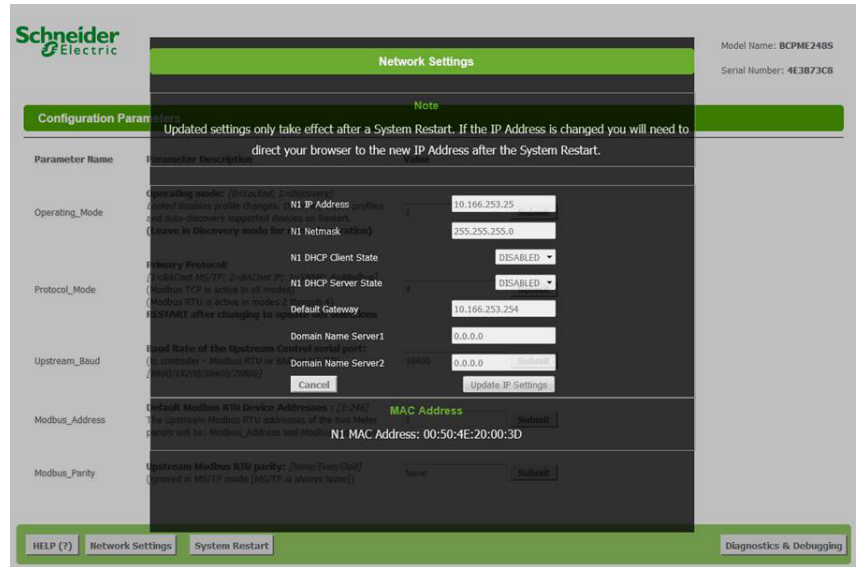
Using the GUI to set up the IP address

1. Access the GUI according to the instructions in the "Accessing the Graphical User Interface (GUI)" section. To set IP address parameters, click the button labeled "Network Settings."



The Network Settings screen appears.

Have the desired IP settings ready in advance (contact the system administrator). IP parameters for use with BACnet IP are static, not dynamic.



2. Set the IP address for use on the BACnet/IP network:
 - a. Enter the desired IP address in the N1_IP_Address field (in the format xxx.xxx.xxx.xxx)
 - b. If necessary, change the Subnet Mask by entering the appropriate new value in the N1_Netmask field
 - c. If the BCPMSCE is connected to an Ethernet gateway, enter its IP address in the Default Gateway field. This is especially critical if the BCPMSCE will be used as a BACnet BBMD device.
 - d. Click the Update IP settings button. The BCPMSCE changes its settings.
 - e. Click the System Restart button and wait for the BCPMSCE to fully initialize. The GUI will connect when the BCPMSCE is installed on a network that matches the settings and the new IP address is entered into a web browser on a PC properly configured for the network. .

Using the GUI to Configure the Communication Protocols

Access the GUI according to the instructions in the “Accessing the Graphical User Interface (GUI)” section.

Parameter Name	Parameter Description	Value
Operating_Mode	Operating mode: [0=Locked; 1=Discovery] <i>Locked</i> disables profile changes. <i>Discovery</i> clears profiles and auto-discovers supported devices on Restart. (Leave in Discovery mode for normal operation)	1 <input type="button" value="Submit"/>
Protocol_Mode	Primary Protocol: [1=BACnet MS/TP; 2=BACnet IP; 3=SNMP; 4=Modbus] (Modbus TCP is active in all modes) (Modbus RTU is active in modes 2 through 4) RESTART after changing to update GUI selections	4 <input type="button" value="Submit"/>
Upstream_Baud	Baud Rate of the Upstream Control serial port: (to controller - Modbus RTU or BACnet MS/TP) [9600/19200/38400/76800]	19200 <input type="button" value="Submit"/>
Modbus_Address	Default Modbus RTU Device Addresses : [1->16] The Upstream Modbus RTU addresses of the two Meter panels will be: Modbus_Address and Modbus_Address+1	1 <input type="button" value="Submit"/>
Modbus_Parity	Upstream Modbus RTU parity: [None/Even/Odd] (ignored in MS/TP mode [MS/TP is always None])	Even <input type="button" value="Submit"/>

HELP (?) Network Settings System Restart Diagnostics & Debugging

The home screen on the GUI provides fields for configuration of the BCPMSCE. The BCPMSCE has four primary modes of operation, each of which support a different combination of protocols. Each option field has a Submit button to the right. When changing the value in any field, click Submit to store the new value. The GUI prompts the user to restart the system. If multiple values are changed, it is easiest to submit all changes and restart only once when finished with the whole screen. To restart, click the System Restart button in the row at the bottom of the screen. The restart takes several seconds, during which the server may lose its connection. Messages appear at the top of the screen indicating current status, but do not perform any actions. Simply allow the tool to complete the restart cycle.

The first selection in the GUI is Operating_Mode, which has two choices:

- a. Locked: used for all normal product operation. It is provided as a tool for high-level technical support. The gateway retains its current profile configuration when powered.
- b. Discovery mode (default): deletes profiles and rediscovers them when the device is powered again. The results are the same, unless the profile configuration is intentionally altered. Profile selection and discovery are especially important when using BACnet or SNMP protocols. For normal operation, always use discovery mode.

The second selection in the GUI is Protocol_Mode, used to select the combination of protocols the product communicates with. The BCPMSCE supports five protocols, some of which can operate simultaneously. The table below shows what protocols are supported in each mode.

Protocol Mode	Primary Protocol	Ethernet Protocol	RS-485 Protocol
1	BACnet MS/TP	Modbus TCP	BACnet MS/TP
2	BACnet IP	BACnet IP/Modbus TCP	Modbus RTU
3	SNMP	SNMP/Modbus TCP	Modbus RTU
4	Modbus	Modbus TCP	Modbus RTU

To select a primary protocol mode, enter the corresponding number into the text field adjacent to the Primary Protocol option and click the Submit button to the right of the text field. A prompt appears at the top of the screen instructing the user to restart the system. When finished, the screen refreshes itself with the appropriate fields for the selected mode.

The next GUI selection, in any protocol mode, is the Upstream_Baud rate selection. If you have selected BACnet MS/TP (mode 1) as the primary protocol mode, this value sets the MS/TP baud rate. If you have selected modes 2 or 3 as the primary protocol mode, you may not be using the RS-485 interface at all. If so, this setting can be ignored.

If you have selected BACnet IP, SNMP or Modbus mode, the next selection is Modbus_Parity, which sets the parity of the upstream serial connection. If using Modbus RTU protocol, set this to match your Modbus master. If not, ignore this field.

The following sections show the field selections (with factory default values) specific to each of the four Protocol_Modes.

1. BACnet MS/TP mode

Schneider Electric Model Name: BCPME24BS
Serial Number: 4E3B73CB

Configuration Parameters

Parameter Name	Parameter Description	Value
Operating_Mode	Operating mode: [0=Locked; 1=Discovery] Locked disables profile changes. Discovery clears profiles and auto-discovers supported devices on Restart. (Leave in Discovery mode for normal operation)	1 <input type="button" value="Submit"/>
Protocol_Mode	Primary Protocol: [1=BACnet MS/TP; 2=BACnet IP; 3=SNMP; 4=Modbus] (Modbus TCP is active in all modes) (Modbus RTU is active in modes 2 through 4) RESTART after changing to update GUI selections	1 <input type="button" value="Submit"/>
Upstream_Baud	Baud Rate of the Upstream Control serial port: (to controller - Modbus RTU or BACnet MS/TP) [9600/19200/38400/76800]	19200 <input type="button" value="Submit"/>
DeviceID_Offset	Default BACnet Device ID numbers: [0-4194302] The Virtual Router Device ID = the DeviceID_Offset. The Device ID of a Meter at Modbus address 1 will be DeviceID_Offset+1	27000 <input type="button" value="Submit"/>
Virt_Router_Net	BACnet network number of the Virtual Router: [1-65534] This network number must be DIFFERENT than all other networks in your BACnet enterprise.	27 <input type="button" value="Submit"/>
MSTP_Max_Master	BACnet MS/TP Max Master value: [1-127]	127 <input type="button" value="Submit"/>
MSTP_MAC_Addr	BACnet MS/TP MAC address: [1-127]	1 <input type="button" value="Submit"/>
RTC_Control	Real Time Clock sync mechanism: [0=BACnet Time Sync; 1=Modbus writes] Select which protocol has write access to the RTC.	0 <input type="button" value="Submit"/>

Active profiles

Nr	Node ID	Current profile	Parameters
1	1	Schneider BCPME (BACnet Time Sync) MSTP	<input type="button" value="Remove"/>
2	2	Schneider BCPME (BACnet Time Sync) MSTP	<input type="button" value="Remove"/>

The first three options are discussed previously.

The DeviceID_Offset parameter is used to assign Device_IDs on power-up or on restart until they have been overwritten via BACnet. Enter your desired value here and click submit. The new value is first used at the next power-up or system restart. Valid Device_ID numbers range from 1 to 4194303. Since the numbers assigned during discovery are the sum of the Offset and the Modbus address (which can be any value from 1-247), the Offset values entered in the GUI must be no larger than 4194057.


The BCPMSCE gateway creates a BACnet virtual router and separate BACnet devices for each 42-channel meter panel behind this virtual router, allowing the devices to be discoverable and independently accessed via BACnet, even if the virtual router is connected by MS/TP, using a single MAC address. To use this product with MS/TP, the BACnet system must support the discovery and use of a BACnet router on the MS/TP trunk and any devices beyond it. This virtual router creates an exclusive BACnet network on which the meter's BACnet devices reside. This network must have a BACnet network number that is different from any other networks in the entire BACnet enterprise. When multiple BCPMSCE products are added anywhere in the enterprise, each one must have a unique network number. Failure to set an exclusive value in this field causes communication conflicts in the BACnet system.

Enter a non-conflicting value here and click submit. Valid network numbers range from 1 to 65534; if other values are entered, the network number defaults to 5. The new value is first used at the next power-up or system restart. If using an external BACnet router to connect the BCPMSCE as an MS/TP device, it is recommended that the router also be restarted after the BCPMSCE has completed discovery, when the network number is changed.

The next field for the BACnet MS/TP protocol mode is the `MSTP_Max_Master`, which allows this value to be set prior to using BACnet software to access the BCPMSCE. The default value of 127 works regardless of the addresses the MS/TP network uses, but selecting a lower value may optimize the network. Do not set this value lower than the highest address on the network. To set this value via BACnet, write to the `Max_Master` property of the device object for the BCPMSCE's virtual router.

The final field is the `MSTP_MAC_Addr`, which sets the MAC address for the virtual router. The BCPMSCE panel(s) are devices on the internal BACnet network and are not directly addressable as MAC addresses on the MS/TP network.

2. BACnet IP mode



Model Name: BCPME24BS
Serial Number: 4E3B73CB

Configuration Parameters

Parameter Name	Parameter Description	Value
Operating_Mode	Operating mode: [0=Locked; 1=Discovery] <i>Locked</i> disables profile changes. <i>Discovery</i> clears profiles and auto-discovers supported devices on Restart. (Leave in Discovery mode for normal operation)	1 <input type="text"/> <input type="button" value="Submit"/>
Protocol_Mode	Primary Protocol: [1=BACnet MS/TP; 2=BACnet IP; 3=SNMP; 4=Modbus] (Modbus TCP is active in all modes) (Modbus RTU is active in modes 2 through 4) RESTART after changing to update GUI selections	2 <input type="text"/> <input type="button" value="Submit"/>
Upstream_Baud	Baud Rate of the Upstream Control serial port: (to controller - Modbus RTU or BACnet MS/TP) [9600/19200/38400/76800]	19200 <input type="text"/> <input type="button" value="Submit"/>
Modbus_Address	Default Modbus RTU Device Addresses : [1-246] The Upstream Modbus RTU addresses of the two Meter panels will be: Modbus_Address and Modbus_Address+1	1 <input type="text"/> <input type="button" value="Submit"/>
Modbus_Parity	Upstream Modbus RTU parity: [None/Even/Odd] (ignored in MS/TP mode [MS/TP is always None])	Even <input type="text"/> <input type="button" value="Submit"/>
DeviceID_Offset	Default BACnet Device ID numbers: [0-4194302] The Virtual Router Device ID = the DeviceID_Offset. The Device ID of a Meter at Modbus address 1 will be DeviceID_Offset+1	27000 <input type="text"/> <input type="button" value="Submit"/>
Virt_Router_Net	BACnet network number of the Virtual Router: [1-65534] This network number must be DIFFERENT than all other networks in your BACnet enterprise.	27 <input type="text"/> <input type="button" value="Submit"/>
BACnet_IP_Port	BACnet IP port: Default is 47808 (0xBAC0). enter in decimal [1-65535]	47808 <input type="text"/> <input type="button" value="Submit"/>
BBMD_Enable	Enable BBMD support: [Enter <i>BBMD</i> to enable or - (<i>hyphen</i>) to disable] Specify other BBMD devices in a bd.ini file and transfer to unit via Diagnostics & Debugging	- <input type="text"/> <input type="button" value="Submit"/>
RTC_Control	Real Time Clock sync mechanism: [0=BACnet Time Sync; 1=Modbus writes] Select which protocol has write access to the RTC.	0 <input type="text"/> <input type="button" value="Submit"/>

Active profiles

Nr	Node ID	Current profile	Parameters
1	1	Schneider BCPME (BACnet Time Sync) IP	<input type="button" value="Remove"/>
2	2	Schneider BCPME (BACnet Time Sync) IP	<input type="button" value="Remove"/>

HELP (?)

Network Settings

System Restart

Diagnostics & Debugging

BACnet IP mode uses the same DeviceID_Offset and Virt_Router_Net parameters described above for BACnet MS/TP mode. One additional parameter, BACnet_IP_Port, is used to set the UDP port. Most BACnet systems use the default port (47808 decimal, 0xBAC0 hex) that is recommended in the BACnet standard as the only UDP port. Some large systems need to segment the enterprise and use more than port. If so, enter the number of the port you need to use to access this device. BACnet IP mode does not use MSTP_Max_Master or MSTP_MAC_Ad

3. SNMP mode

Model Name: BCPME248S
Serial Number: 4E3B73C8

Configuration Parameters

Parameter Name	Parameter Description	Value
Operating_Mode	Operating mode: [0=Locked; 1=Discovery] <i>Locked</i> disables profile changes. <i>Discovery</i> clears profiles and auto-discovers supported devices on restart. (Leave in Discovery mode for normal operation)	1 <input type="button" value="Submit"/>
Protocol_Mode	Primary Protocol: [1=BACnet MS/TP; 2=BACnet IP; 3=SNMP; 4=Modbus] (Modbus TCP is active in all modes) (Modbus RTU is active in modes 2 through 4) RESTART after changing to update GUI selections	3 <input type="button" value="Submit"/>
Upstream_Baud	Baud Rate of the Upstream Control serial port: (to controller - Modbus RTU or BACnet MS/TP) [9600/19200/38400/76800]	19200 <input type="button" value="Submit"/>
Modbus_Address	Default Modbus RTU Device Addresses: [1-246] The Upstream Modbus RTU addresses of the two Meter panels will be: Modbus_Address and Modbus_Address+1	1 <input type="button" value="Submit"/>
Modbus_Parity	Upstream Modbus RTU parity: [None/Even/Odd] (ignored in MS/TP mode [MS/TP is always None])	Even <input type="button" value="Submit"/>
Read_Community	SNMP Read Community string: [character string]	public <input type="button" value="Submit"/>
Write_Community	SNMP Write Community string: [character string]	private <input type="button" value="Submit"/>
Trap_Community	SNMP Notification Trap Community string: [character string]	trap <input type="button" value="Submit"/>
SNMP_Notif_IP	Address of the SNMP Notification client: [xxx.xxx.xxx.xxx]	192.168.1.67 <input type="button" value="Submit"/>

Active profiles

Nr	Node ID	Current profile	Parameters
1	1	Schneider Electric BCPME SNMP	<input type="button" value="Remove"/>
2	2	Schneider Electric BCPME SNMP	<input type="button" value="Remove"/>

SNMP mode uses four unique parameters. SNMP Community strings are used to control access to the device. Whatever values are entered here must be used in the MIB browser or SNMP access software to communicate with this device. The Read_Community string is used to enable reading data. The Write_Community string is used to enable writing data. The Trap_Community string is used to enable the receipt of event notifications.

The last parameter, SNMP_Notif_IP will be used to set the IP address of the client that used to receive SNMP event notifications for over-threshold events.

Operating the BCPMSCE

Restart the BCPMSCE by using the button at the bottom of the GUI or by cycling the power. It takes about 30 seconds to initialize completely and be ready for external communication.

Commissioning

Commission the BCPMSCE for operation using ION Setup software. See the ION Setup Configuration Guide for instructions.

BACnet Network Management

BACnet configuration uses two default settings that might need to be changed, depending on the application.

- a. Virtual router network ID number.** Every logical network segment (IP subnet, MS/TP trunk, etc.) in an entire system must have a (16-bit) network ID number that is unique from all other BACnet networks in the enterprise. The BACnet network administrator assigns this network ID so that no two ID numbers conflict (whether using BACnet/IP or MS/TP). Within each segment, every device is physically identified by the combination of its 8-bit MAC address and the 16-bit network ID number.

To support multiple meter panels (panel 1 and panel 2 are separate) with a single gateway, the BCPMSCE creates a virtual BACnet router that presents multiple BACnet devices using a single (its own) MS/TP MAC address. Each BCPMSCE must have its own (internal) network ID, and it creates a device object for itself and one for each Modbus address discovered.

The factory default network address is 50 (decimal). If that number is already in use in the system, assign a unique address using the graphical user interface (GUI) on the built-in web server (this requires an Ethernet connection to a web browser; see BACnet/IP Setup section for instructions on changing configuration settings using the GUI). Valid network numbers range from 1 to 65534; if other values are entered, the network number defaults to 5.

b. Device_ID Offset. Every BACnet device must have a BACnet Device_ID number that is unique throughout the entire enterprise. Since the BCPMSCE presents every Modbus meter as a BACnet device, each connected meter that has a Modbus address must have a BACnet Device_ID.

By default, each device discovered receives a Device_ID number that is the sum of an offset value (default is 50000) and the Modbus address of the device. If these Device_ID numbers cause a conflict with existing devices in the system, or if the system includes multiple BCPMSCEs, change the Device_ID numbers before connecting the BCPMSCE to the system. This can be managed one of two ways:

- i. Connect to the BCPMSCE directly (offline from the system) with the devices (meters). After the BCPMSCE discovers the devices and assigns their default ID numbers, the user can choose new Device_ID values and write these to each device using BACnet software. Subsequent discoveries will not overwrite these values with defaults even if the BCPMSCE is then set to Discovery mode.
- ii. Use the GUI on the built-in web server to modify the offset value used to calculate default Device_IDs in the discovery process (this requires an Ethernet connection to a web browser; see BACnet/IP Setup section for instructions on changing configuration settings using the GUI). The BCPMSCE retains this offset value and uses it to assign Device_ID numbers every time power is cycled if the BCPMSCE is in Discovery mode. Valid Device_ID numbers range from 1 to 4194303. Since the numbers assigned during discovery are the sum of the Offset and the Modbus address (which can be any value from 1-247), any Offset values entered in the GUI must be less than 4194057.

BACnet PICS (Protocol Implementation Conformance Statement)

Vendor Name: Schneider Electric

BACnet Vendor ID 335

Product Name: BCPMSCE Series Branch Circuit Monitor

Product Model Number: <Model Number>

Product Description: Branch Circuit Monitor

BACnet Protocol Version: Version 1 Revision 12

BACnet Standardized Device Profile (Annex L) – [Note: BCPMSCE incorporates a gateway device]

- BACnet Application Specific Controller (B-ASC)

BACnet Interoperability Building Blocks Supported (Annex K):

- K.1.2 BIBB - Data Sharing - ReadProperty-B (DS-RP-B)
- K.1.4 BIBB - Data Sharing - ReadPropertyMultiple-B (DS-RPM-B)
- K.1.8 BIBB - Data Sharing - WriteProperty-B (DS-WP-B)
- K.1.10 BIBB - Data Sharing - WritePropertyMultiple-B (DS-WPM-B)
- K.1.12 BIBB - Data Sharing - COV-B (DS-COV-B)
- K.2.2 BIBB - Alarm and Event-Notification Internal-B (AE-N-I-B)
- K.2.5 BIBB - Alarm and Event-ACK-B (AE-ACK-B)
- K.2.11 BIBB - Alarm and Event-Information-B (AE-INFO-B)
- K.5.2 BIBB - Device Management - Dynamic Device Binding-B (DM-DDB-B)
- K.5.4 BIBB - Device Management - Dynamic Object Binding-B (DM-DOB-B)
- K.5.6 BIBB - Device Management - DeviceCommunicationControl-B (DM-DCC-B)
- K.5.12 BIBB - Device Management - TimeSynchronization-B (DM-TS-B)
- K.5.22 BIBB - Device Management – List Manipulation-B (DM-LM-B)
- K.5.20 BIBB – Device Management-Restart-B (DM-R-B)

Standard Object Types Supported

- Device Object
- Analog Input
- Analog Output
- Analog Value

Unsupported Properties and Restrictions

- Does not support BACnet CreateObject
- Does not support BACnet DeleteObject
- Does not support any proprietary properties
- No proprietary properties exist
- No range restrictions exist
- Max_Master is writable

Data Link Layer Options

- BACnet IP, (Annex J)
- MS/TP master (Clause 9), baud rate up to 76.8 kbps

Networking Options

- BACnet/IP Broadcast Management Device (BBMD)
- Registrations by Foreign Devices

Character Sets Supported

- ISO 10646 (UTF-8) / ANSI X3.4

General BACnet Programming Information

The BCPMSCE consists of a BACnet virtual router and one or two 42-channel branch circuit meters. The BACnet virtual router has its own device object and an internal BACnet network. The branch circuit monitors have their own device objects that are logical devices on the network internal to (beneath) the virtual router. It is critical that the network number of the virtual router's internal network be different than any other network number in your entire BACnet system. The network number is set to 50 at the factory, but can be changed in the GUI or by writing to the Present_Value of the AV2 data object associated with that device. Changes to the network number do not take effect until the BCPMSCE is re-started, either from the GUI or by cycling the power.

The default Device ID of the virtual router is the Device_Offset parameter which is set to 5000 at the factory, but can be changed in the GUI or by writing to Present_Value of the AV1 data object associated with that device. Changes to the network number do not take affect until the BCPMSCE is re-started, either from the GUI or by cycling the power. The default Device IDs are numbered to consecutively follow the Device ID of the virtual router (e.g. if the Device_Offset parameter is 50000, the virtual router has a Device_ID of 50000, the branch circuit monitor called Panel 1 has a Device_ID of 50001 and the branch circuit monitor called Panel 2 (if present) has a Device_ID of 50002.

All Device_IDs are writable. Once a device's Object_Identifier is overwritten, changes to the ID Offset no longer affect that Object_Identifier, even in Discovery mode. Make further changes to the value by writing the Object_Identifier property.

The default Object_Name property value of each device object is an abbreviated name of the meter series discovered with an underscore and the Modbus address of the meter appended to it. The Object_Name is a writable property. Once a device's Object_Name is overwritten, the Object_Name does not revert to the initial default, even in Discovery mode. Make further changes to the value by writing the Object_name property.

The BCPMSCE supports Subscribe_COV, with default COV increment values assigned as shown in the data object tables. If these values are not appropriate for a specific application, write them as needed when they are subscribed. On subsequent power cycles, no subscriptions are active and the COV increments return to their default values.

Data values written to AV objects are accepted (without error) by the data object and passed through to the corresponding Modbus register. There is no direct indication via the BACnet protocol if invalid values are rejected. After an invalid value is written to the Present_Value of an AV, subsequent reads of that property return the new (invalid) value until the next time the BCPMSCE refreshes its data (this may take several seconds).

BBMD Support

When the BCPMSCE is in BACnet IP mode, it can be configured as a BACnet Broadcast Management Device (BBMD) by adding devices to a comma separated value text file named bdt.ini, and loading it onto the device. The example below shows the syntax required. All lines beginning with two forward slashes are interpreted as comments. Use exactly one line per device, separated by commas (no spaces). Once edited, upload the bdt.ini file to the gateway through the GUI. Click the <Diagnostics and Debugging> button in the lower right corner of the GUI and follow the folder tree under Navigation to the following folder: "Schneider Electric BCPM Series Gateway/Setup/ File Transfer." Select the "General" tab (this is important - using the wrong tab can overwrite critical files). Click the <Browse> button and select your bdt.ini file. Then click <Submit>. The GUI should quickly indicate "The file was updated successfully." Click the <System Restart> button, click <OK> on the confirmation dialog and wait for the gateway to reinitialize (takes about 30 seconds). BBMD changes are made by uploading a new bdt.ini file.

```
// Bdt.ini

// The format of this table must be (without the forward slashes - they are
comment indicators):

//

//BBMD IP_Address , BBMD port , BBMD subnet Mask

//

147.26.116.217,47808,255.255.255.255

172.16.17.198,47808,255.255.255.255
```

General SNMP Programming Information

The BCPMSCE can be configured to support the SNMP V2c protocol over Ethernet. The SNMP community string and the IP address for the client receiving SNMP V2c event notifications can be set via the GUI. MIB files are available for download from the BCPM Downloads and Documents page at www.se.com to enable accessing the BCPMSCE from an MIB browser.

The BCPMSCE OID structure organizes the data under two “panels” representing the two breaker panels that can be monitored by a fully populated BCPMSCE. Panel 1 corresponds to the CT strips connected to the “Panel 1A” and “Panel 1B” connectors and to the data set under Modbus address 1 or BACnet device identified as Node_1 in the GUI. Panel 2 corresponds to the CT strips connected to the “Panel 2A” and “Panel 2B” connectors and to the data set under Modbus address 2 or BACnet device identified as Node_2 in the GUI.

For each panel, data is arranged under six tree branches.

- The Configuration branch contains all writable configuration parameters.
- The Alarms branch contains all the event notification traps, the global event status registers and counters and tables of the event status indicators.
- The Voltage Inputs branch contains all data measurements pertaining to the voltage inputs.
- The Auxiliary Inputs branch contains all data measurements pertaining to the aux inputs other than voltage-related.
- The Branch Inputs branch contains all data measurements to the branch inputs in table format.
- The Flex Circuits branch contains all data measurements to the logical meter summaries in table format.

Cybersecurity

Overview


This chapter contains up-to-date information about your product's cybersecurity. network administrators, system integrators and personnel that commission, maintain or dispose of a device should:

- Apply and maintain the device's security capabilities. See "*Device security capabilities*" for more details.
- Review assumptions about protected environments. See "*Protected environment assumptions*" for more details.
- Address potential risks and mitigation strategies. See "*Potential Risks and compensating controls*" for more details.
- Follow recommendations to optimize cybersecurity.

Your device has security capabilities that:

- Allow it to be part of a NERC CIP compliant facility. Go to the North American Electric Reliability Corporation website for information on NERC Reliability Standards.
- Align with cybersecurity standards in the IEC 62443 international standard for business IT systems and Industrial Automation and Control Systems (IACS) products. Go to the International Electrotechnical Commission website for information about the IEC 62443 international standard.

To communicate a security topic affecting a Schneider Electric product or solution, go to www.se.com/en/work/support/cybersecurity/vulnerabilitypolicy.jsp.

 WARNING
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY
<ul style="list-style-type: none">• Change default passwords to help prevent unauthorized access to device settings and information.• Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.• Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).• Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.
Failure to follow these instructions can result in death, serious injury, or equipment damage.

Product defense-in-depth

Use a layered network approach with multiple security and defense controls in your IT and control system to minimize data protection gaps, reduce single-points-of-failure and create a strong cybersecurity posture. The more layers of security in your network, the harder it is to breach defenses, take digital assets or cause disruption.

Device security capabilities

This section describes the security capabilities available with your device.

User accounts

These security capabilities help enforce authorizations assigned to users, segregation of duties and least privilege:

- User authentication is used to identify and authenticate software processes and devices managing accounts.
- Device configuration and security communications configuration.

Hardening

These security capabilities help prohibit and restrict the use of unnecessary functions, ports, protocols and/or services:

- Least functionality can be applied to prohibit and restrict the use of unnecessary functions, ports, protocols and/or services.
- Port numbers can be changed from default values to lower the predictability of port use.

Protected environment assumptions

- Cybersecurity governance – available and up-to-date guidance on governing the use of information and technology assets in your company.
- Perimeter security – installed devices, and devices that are not in service, are in an access-controlled or monitored location.
- Emergency power – the control system provides the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.
- Firmware upgrades – device upgrades are implemented consistently to the current version of firmware.
- Controls against malware – detection, prevention and recovery controls to help protect against malware are implemented and combined with appropriate user awareness.
- Physical network segmentation – the control system provides the capability to:
 - Physically segment control system networks from non-control system networks.
 - Physically segment critical control system networks from non-critical control system networks.
- Logical isolation of critical networks – the control system provides the capability to logically and physically isolate critical control system networks from non-critical control system networks. For example, using VLANs.
- Independence from non-control system networks – the control system provides network services to control system networks, critical or non-critical, without a connection to non-control system networks.
- Encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.
- Zone boundary protection – the control system provides the capability to:
 - Manage connections through managed interfaces consisting of appropriate boundary protection devices, such as: proxies, gateways, routers, firewalls and encrypted tunnels.

- Use an effective architecture, for example, firewalls protecting application gateways residing in a DMZ.
- Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site, for example, data centers.
- No public internet connectivity – access from the control system to the internet is not recommended. If a remote site connection is needed, for example, encrypt protocol transmissions.
- Resource availability and redundancy – ability to break the connections between different network segments or use duplicate devices in response to an incident.
- Manage communication loads – the control system provides the capability to manage communication loads to mitigate the effects of information flooding types of DoS (Denial of Service) events.
- Control system backup – available and up-to-date backups for recovery from a control system failure.

Potential risks and compensating controls

Address potential risks using these compensating controls:

Area	Issue	Risk	Compensating controls
User accounts	Default account settings are often the source of unauthorized access by malicious users.	If you do not change the default password, unauthorized access can occur.	Change the default password to help reduce unauthorized access.
Secure protocols	Modbus TCP, BACnet/IP and SNMP protocols are unsecure. The device does not have the capability to transmit encrypted data using these protocols.	If a malicious user gained access to your network, they could intercept communications.	For transmitting data over an internal network, physically or logically segment the network. For transmitting data over an external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.

Default security settings

Area	Setting	Default
Communication protocols	Modbus TCP	Enabled
	BACnet/IP	Disabled
	SNMP	Disabled

Passwords

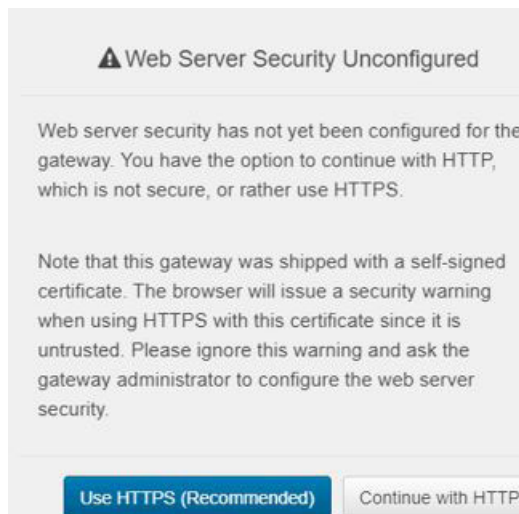
Recommendations to optimize cybersecurity in a protected environment:

- Document and store passwords and usernames in a protected location.
- Change the default password to help reduce unauthorized access. Default account settings are often the source of unauthorized access by malicious users.
- Use complex passwords or passphrases.
- Follow user account management tasks as described by your organization or contact your network administrator, for example, maximum password age or history policies.

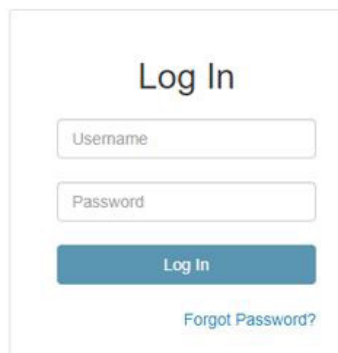
Default password and user accounts

Accessing the GUI for the first time with firmware version 1.027 or higher

Open the web browser and enter the IP address of the BCPMSCE into the address/URL field on the browser. Press enter. A "**Web Server Security Unconfigured**" warning message screen appears. Read the instructions carefully before you click the "**Use HTTPS (Recommended)**" button.



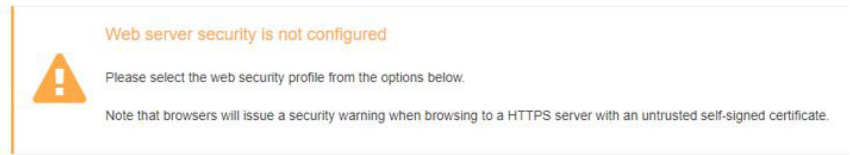
A "**Your connection is not private**" warning message screen appears. Click the "**Advanced**" button on the bottom left corner of the warning message screen. Click the underlined text "**Proceed to xx.xx.xx.xx (unsafe)**" link. The "**Log In**" screen appears. Enter the "**Username**" and "**Password**".



Default account settings:

Username	Password
admin	<p>Password is unique for each device. You need to enter the default alphanumeric password on the barcode label which is affixed to the metal enclosure of the product. Format of default password barcode label: For eg: dX2oO8\$A%e94SVoX</p> <p>NOTE: It is recommended for the users to change the default factory-set password to a complex password after logging to the GUI.</p>

On the first login to the GUI, the "**Web sever security is not configured**" warning message screen appears. Read the instructions carefully before you select the "**Mode**" in the warning message.



Mode

- HTTPS with own trusted TLS certificate (**recommended** and most secure)
- HTTPS with default untrusted self-signed TLS certificate (vulnerable to man-in-the-middle attack)
- HTTP with built-in payload encryption (vulnerable to man-in-the-middle attack)

Save

Click the "**HTTPS with own trusted TLS certificate (recommended and most secure)**" mode. Once this mode is selected, the user can drag and drop their own "**SSL Certificate**" and "**Private Key**" files into their respective fields. If the "**Private Key**" is encrypted, specify this in "**Private Key Passphrase**" field. Click "**Save**" button.

Mode

- HTTPS with own trusted TLS certificate (**recommended** and most secure)
- HTTPS with default untrusted self-signed TLS certificate (vulnerable to man-in-the-middle attack)
- HTTP with built-in payload encryption (vulnerable to man-in-the-middle attack)

Certificate

Private Key

Private Key Passphrase

Save

A "**Redirecting**" message will appear and after a short period of time the GUI "**Configuration Parameters**" screen will open.

If you do not have a trusted TLS certificate, click the "**HTTPS with default untrusted self-signed TLS certificate (vulnerable to man-in-the-middle attack)**" mode.

A "**Redirecting**" message will appear and after a short period of time the GUI "**Configuration Parameters**" screen will open.

Changing passwords

NOTICE

LOSS OF ACCESS

- Record your device's user and password information in a secure location.

Failure to follow these instructions can result in data loss and loss of access to the device.

NOTICE

LOSS OF DATA OR PRODUCT CONFIGURATION

- Do not let unauthorized personnel gain physical access to the device.

Failure to follow these instructions can result in data loss and loss of access to the device.

After logging to the GUI for the first time, it is recommended to change the default factory-set password.

In the "*Configuration Parameters*" window, click the button labelled "*Diagnostics & Debugging*". The "*Navigation*" window appears.

On the "*Navigation*" window, under the product gateway, click "*Setup*". Navigate to "*User Management*". Click the "*Password*" tab.

Enter the new alphanumeric complex password in the "*Password*" and "*Confirm Password*" fields. Click "*Confirm*" to save the changes.

To confirm the changes, click the "*Logout*" button and access the GUI with the new password.

Harden the device

Recommendations to optimize cybersecurity in a protected environment:

- Harden the device according to your company policies and standards.
- Review assumptions about protected environments and address potential risks and mitigation strategies. See "*Product defense-in-depth*" for more details.
- Change the default passwords/passcodes. See "*Changing passwords*" for more details.
- Change the communication protocol ports from their default values. This lowers the predictability of port use.
- Disable communication protocol ports when they are not in use. This reduces the attack surface.

Firmware upgrades

When device firmware is upgraded – security configuration remains the same until changed, including usernames and passwords/passcodes. It is recommended to review security configuration after an upgrade to analyze privileges for new or changed device features and revoke or apply them according to your company policies and standards.

Secure disposal guidelines

Use the *Secure disposal checklist* when disposing a device to help prevent potential disclosure of data.

Secure disposal checklist

Record activities: Document disposal actions according to your company policies and standards to keep a record of activities.

Decommission related rules and sanitize records:

- Follow decommission and sanitization tasks as described by your organization or contact your network administrator.
- Decommission network and security rules, e.g. a firewall rule that could be used to get past the firewall.
- Perform records tracking sanitization tasks to remove records in related systems, e.g. monitoring SNMP servers.

Disposal and reuse: See *Disposal, reuse, recycling*, for more details.

Disposal, reuse, recycling

Before removing the device from its intended environment, follow the *Secure disposal guidelines* in this document.

Follow device removal tasks described by your organization or contact your network administrator to determine a responsible method of disposal.

Dispose the device according to the legislation of the country. Some regulatory organizations include:

- The United States *Environmental Protection Agency (EPA)* for guidance on the sustainable management of electronics.
 - The EPA provides an *Electronic Product Environmental Assessment Tool (EPEAT)* that helps assess the environmental attributes of electronics.
- The European *Waste Electrical & Electronic Equipment Directive (WEEE Directive)* is the *community directive on waste electrical and electronic equipment*.
- The European *Restriction of Hazardous Substances Directive (RoHS)* directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

NOTICE

UNAUTHORIZED OR UNINTENDED ACCESS TO CONFIDENTIAL DATA

- Store devices that are not in service in an access-controlled or monitored location.
- Physically destroy devices that are decommissioned.

Failure to follow these instructions can result in unauthorized or unintended access to sensitive or secure customer data.

Device disposal

It is recommended that the entire device is physically destroyed. Destroying the device helps prevent potential disclosure of data contained in the device that was not removed.

Device reuse

Store the device in a location that is access controlled or monitored if there is potential for reuse.

Device recycling

Go to www.se.com and search for the Product Environmental Profile for your device type to get instructions on managing e-waste.

Troubleshooting

Table 5: Troubleshooting guide

Problem	Solution
Product is not communicating over Modbus daisy chain	<ul style="list-style-type: none">• Check the unit Modbus address to ensure that each device on the daisy chain has a unique address.• Check Parity.• Check the communications wiring.• Check that the daisy chain is properly terminated.
Power factor reading is not as expected	<ul style="list-style-type: none">• Verify voltage taps are connected in appropriate phase rotation.• Verify strip configuration register matches actual strip installation.• Verify phase rotation of breakers
Current reading is not as expected, or reading is on different CT number than expected	<ul style="list-style-type: none">• Verify strip configuration register matches actual strip installation.• Verify ribbon cable is fully seated and in the correct orientation.
Current is reading zero, even when small currents are still flowing through circuit	<ul style="list-style-type: none">• The product cuts off at 50 mA, and will set the reporting register to 0 mA for currents near or below this range.

China RoHS Compliance Information

Table 6: EFUP Table

部件名称 Part Name	有害物质 - Hazardous Substances					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr (VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
电子件 Electronic	X	0	0	0	0	0

本表格依据SJ/T11364的规定编制。

O: 表示该有害物质在该部件所有均质材料中的含量均在GB/T 26572规定的限量要求以下。

X: 表示该有害物质至少在该部件的某一均质材料中的含量超出GB/T 26572规定的限量要求。

(企业可在此处，根据实际情况对上表中打“X”的技术原因进行进一步说明。)

This table is made according to SJ/T 11364.

O: indicates that the concentration of hazardous substance in all of the homogeneous materials for this part is below the limit as stipulated in GB/T 26572.

X: indicates that concentration of hazardous substance in at least one of the homogeneous materials used for this part is above the limit as stipulated in GB/T 26572

Z000057-0B

Schneider Electric
35, rue Joseph Monier
92500 Rueil Malmaison
France
+ 33 (0) 1 41 29 70 00
www.se.com

As standards, specifications, and designs change from time to time, please ask for confirmation of the information given in this publication.

© 2020 Schneider Electric. All Rights Reserved.

Z206857-0C 04/2020