SER^{NET}

Sequence of Events Recorder

Installation & Operation Manual

Document no. 1087-147E

Table of Contents

Scope

This manual describes the functions, features, installation, and configuration of SER^{NET}. This includes usage of the Web browser interface.

Chapter 1 Product Overview

SER^{NET} is an advanced alarm management system that captures critical alarms with 1 ms precision in the sequence they occur for quick determination of the root cause. The SER^{NET} can display your alarms in a WEB Browser for easy analysis and provides real time data outputs via serial and Ethernet ports, making it ideal for monitoring your critical alarms from substation switchgear, transformers, turbines, boilers, pumps, motors, UPS, HVAC, building security and more.

Each SER^{NET} product can work as a stand-alone system monitoring up to 48 digital inputs. If the unit is ordered with 61850 the unit will have an equal quantity of IEC61850 points as well. Multiple SER^{NET} units can be networked together to form a larger system with all events consolidated in one chronological list as they occur. You can configure status reports in a variety of ways as explained later in this manual.

Model Number Codes / Ordering Information

	# Inputs and Mounting		Power	Field Contact Voltage (FCV)	Options
	Code	Description			
SER^{NET}	48-RK	48 input 19" Rack	1F = 24 Vdc 1U = Universal AC/DC 120/240 Vac or 125 Vdc 2F = Dual 24 Vdc 2U = Dual AC/DC UF = AC/DC & 24 Vdc	X = 24 Vdc Internally provided D = 125 Vdc Externally provided C = 24-125 Vdc Customer specified Y = 120 Vac Customer supplied Option X on Models: RK, SD, RK1, ICR1, SD1 Option Y on Models: RK2, ICR2, SD2	MOD = Modbus Protocol DNP = DNP Protocol MWEB = Alarms from multiple units (max 24) can be collected on one SERNET for common display, event log, printing 61850 = IEC 61850 Protocol
	16-SD	16 input Surface/ DIN Rail mounting			
	32-SD	32 input Surface/ DIN Rail mounting			
	48-SD	48 input Surface/ DIN Rail mounting			
	32-RK1	32 input 19" Rack mount, 1 ½ term/input			
	32-RK2	32 input 19" Rack mount, 2 term/input (AC Input)			
	32-RK3	32 input 19" Rack mount, 2 term/input (DC Input)			
	32-ICR1	32 input ISM Card Rack, 1 ½ term/input			
	32-ICR2	32 input ISM Card Rack, 2 term/input (AC Input)			
	32-ICR3	32 input ISM Card Rack, 2 term/input (DC Input)			
	32-SD1	32 input Surface/DIN Rail mount, 1 ½ term/input			
	32-SD2	32 input Surface/DIN Rail mount, 2 term/input (AC Input)			
	32-SD3	32 input Surface/ DIN Rail mount, 2 term/input (DC Input)			

Sample Model Number

SER^{NET} – _____ – _____ – _____ – _____ – _____

# of Inputs	Mounting	Power	FCV	Options

Typical Model Number for a Single Unit

SER^{NET} – 48-RK-2U-C-MOD-DNP

- 48 Inputs
- 19” Rack
- Dual AC/DC Power Supply
- 20–150 Vdc FCV
- Modbus Protocol
- DNP Protocol

Typical Model Number for 256 Point System

(5) SER^{NET} – 48-SD-2U-C-MOD-DNP

(1) SER^{NET} – 16-SD-2U-C-MOD-DNP-MWEB

- 256 Inputs
- Surface or Din Rail Mounting
- Dual AC/DC Power Supply
- 20–150 Vdc FCV
- Modbus Protocol
- DNP Protocol
- Multiple WEB Browser Display

Features

Inputs

Each SER^{NET} unit can accommodate 16, 32, or 48 digital contact inputs depending on the model. The unit can be configured via the Web Browser for N.O. (Normally Open – contact closes on alarm) or N.C. (Normally Closed – contact opens on alarm).

Models RK, SD, RK1, SD1, and ICR1:

The digital contact inputs can be *dry* (voltage free) using AMETEK supplied Field Contact Voltage (FCV Options X, D) or can be *wet* using customer supplied voltages between 20-150Vdc (FCV Option C).

Models RK2, SD2, and ICR2:

The digital contact inputs are isolated from input to input and are activated by customer supplied 120 Vac FCV. The unit does not provide FCV.

Models RK3, SD3, and ICR3:

The digital contact inputs are isolated from input to input and are activated by customer supplied 20 to 150 Vdc FCV. The unit does not provide FCV.

The SER^{NET} will log all alarms with 1 ms resolution and can be filtered (to prevent false alarms or multiple occurrences) please refer to Chapter 3 for details.

Alarm Memory

Each SER^{NET} unit can store 40,000 events in non-volatile memory. The oldest events will be overwritten once the memory is full (First In, First Out). The following types of events are stored in memory:

Event Types	Event Descriptor	Event Description
Alarm Event	A N	Input goes into the Alarm State Input Returns to Normal State
Diagnostic Event	D	System Diagnostic for: -Unit Configuration -Disabled Alarms (Manual or Automatically) -Acknowledged Alarms -System Watchdog Fault -Communication Errors -Power Supply Failure
Time Event	T	Event Associated with Time Clock -Time Sync enabled -Time Sync lost -Time Reset

Each event will be stored with its own Date/Time stamp to the millisecond, Descriptor, Station ID, Device ID, Input Channel Number (Point) and Event Description. The Alarm Event Description can be configured for separate Alarm Text and Return to Normal text.

Alarm Indicators

Each Alarm input has a corresponding LED indicator that will flash for a point in alarm and turn off when the point returns to normal. At the top of the *Active Alarms* page there is a button, *Acknowledge Alarms*, which, when clicked, changes the flashing LED indicator to solid on. This is explained further in Chapter 3.

Alarm Outputs

SER^{NET} has two configurable Form C contact outputs (Coil State), to indicate various alarm conditions. Each output can be configured with an energized or de-energized coil in the alarm state. Relay Function: the alarm can be configured for:

- Alarm – (Activate when any alarm is active)
- Reflash – (Activate when any alarm is active and de-activate for ½ second for new alarms

- Pulsed Alarm – (Alarm output pulses for every alarm)
- Watchdog – (Activate for an internal system error)
- Horn – (Activate Horn when Alarm is Active)

Time Synchronization

The SER^{NET} can be synchronized externally via:

- IRIG-B – (BNC Connector provided)
- External Serial Time Sync. – (Master/Slave via RS-485 output from another SER^{NET} unit)
- Alternate Time Source – NTP, IEEE 1588 (via RJ45 Ethernet Port) or your PC clock (converted to UTC)
- Manually – (via WEB Browser connected to Ethernet Port)

There is an internal Real Time Clock (RTC) accurate to 1 second per day (0.69ms/minute) in cases where there is no external time sync present.

IRIG-B

Accuracy to +/- 1 ms of UTC time when connected to a high accuracy GPS Clock.

External Serial Time Sync. (unit to unit)

A SER^{NET} unit connected to IRIG-B or NTP can be designated as a 'Master' for interconnection to up to 24 'Slave' SER^{NET} units via a RS-485 serial output. The last slave in the string must be terminated. Please refer to Chapter 3. The slave SER^{NET} units will synchronize to +/- 2ms of the Master.

NTP (Network Time Protocol)

NTP can have an accuracy up to +/- 1 ms of UTC time when connected to a Quantum 2 NTP Time Server. The NTP time sync is provided via the Ethernet port, which is configured to connect to up to three IP addressable high accuracy GPS clocks installed on the network LAN. The GPS clocks query the NTP host and through several transmissions, it is able to synchronize the time. Overall accuracy is dependent on where the NTP Time Server is located on the LAN, number of hops, etc and network traffic. Typical accuracies can be +/- 2ms of UTC time when located in the same LAN as the SER^{net}.

IEEE 1588 (IEEE Precision Time Protocol)

IEEE 1588 can have an accuracy up to +/- 1 ms of UTC time when connected to a IEEE 1588 Time Server. The IEC1588 time sync is provided via the Ethernet port.

Manual Time Set

Accuracy to the same specifications as the PC clock and long term accuracy is maintained via the internal Real-Time Clock (RTC).

Power Supply Options

The SER^{NET} connects directly to a variety of power inputs: 24 Vdc, 125 Vdc, & 120/240 Vac at 50/60Hz. (Other power supply options are available via external power supplies)The SER^{NET} can be equipped with a built-in single power supply or a dual redundant power supply using the same or different power inputs.

There are two power supply versions available for SER^{NET}.

24 Vdc

120/240 Vac or 125 Vdc Universal

The power supplies are removable from the front of the unit with power connections at the back. Each power supply slot is keyed (per order), preventing a 24 Vdc power supply from being inserted into a universal 120 Vac/240 Vac/125 Vdc power supply slot.

PS1, the first slot to the left (when viewed from the front) uses power supply terminal block connections TB3 (9, 10). The second slot, PS2 and terminal block connections TB3 (7, 8), is reserved for dual power options using whatever power option is selected. Chapter 2 contains the wiring diagrams.

The power supplies are hot-swappable. There is no need to power down a system for power supply maintenance. Each supply has a bi-color LED to indicate its status:
Green –power supply is functioning correctly.
Red – power supply should be replaced as soon as possible.
Note: Red LED only operates when using the dual power options

Field Contact Voltage (FCV) Power Supply

The SER^{NET} models RK, SD, RK1, SD1, and ICR1 can internally generate 24 Vdc Field Contact Voltage (FCV) or can accept any customer supplied voltage between 20 and 150 Vdc. There are four terminals provided for FCV connection to the field contact inputs. Refer to Chapter 2 for wiring diagrams.

Models RK2, SD2, and ICR2 require a customer supplied FCV of 120 V ac.

Models RK3, SD3, and ICR3 require a customer supplied FCV of 20-150 V dc.

DC contact inputs operate over the range of 20 to 150 Vdc, and thus require no hardware configuration.

Status Indicators

Two status indicators, adjacent to the Alarm Input Indicators, are provided:

Time Sync:

Green – a valid Time Synchronization (either IRIG-B, NTP or 1588) is present
Red – no Time Sync.

System Status:

Green – system is functioning normally
Red – problem detected

Serial Port

The serial port is a DB-9 female connector. It can be configured for either RS-232 or RS-485 mode. Mode selection is done on the *Serial Communications* page of the Web browser interface. RS-485 termination is internal, and is selected with a checkbox on the Serial Communications and/or Date/Time pages. Details can be found in Chapter 3.

Ethernet

Ethernet communication is provided by an RJ-45 connector. SER^{NET} supports 10 Mbps and 100 Mbps. It also provides support for fixed and DHCP IP addresses. The following Ethernet communications are supported:

Web browser	(configuration and display of alarms)
Modbus TCP/IP	(alarm status, time stamp)
DNP	(alarm status, time stamp)
IEC61850	(alarm status, time stamp)
NTP	(time sync)
1588	(time sync)
Bacnet	(alarm status, time stamp)
SNMP	(Ethernet status)

The Ethernet port allows a minimum of 10 simultaneous connections.

Safety and Agency Approvals

Symbols

Caution, risk of danger. Refer to the Instruction Manual.

Caution, risk of electric shock.

Protective Earth Conductor Terminal

Approvals

SER^{NET} models RK and SD are CE certified for operation under the following conditions:

Indoor Use

Altitude:	Up to 2000 m
Operating Temperature:	–20 to 60 ˚C (–4 to 140 ˚F)
Relative Humidity:	20 – 95 % non-condensing
Transient Over-Voltages	2500 V (Installation or Measurement Category II)
Pollution Degree	2
Equipment Category	Permanently Connected
Operating Voltage Ranges	120/240 Vac, 50/60 Hz 125 Vdc 24 Vdc

SER^{NET} models RK and SD are UL Listed

Chapter 2. Installation & Setup

Safety

Installation and start-up must be performed by trained and qualified personnel. If the unit is not installed and operated as specified, the protection provided by the unit may be impaired.

Before start-up it is important to ensure that:

- The unit can be powered down by a switch, or a circuit breaker, clearly marked as the disconnecting device for the unit. The maximum rating of the disconnecting device is 20 A.
- The disconnecting device is located in close proximity to the unit.
- The equipment is not in a position so that it is difficult to operate the disconnecting device.
- The protective earth terminal is properly connected to protective earth ground.
- The line(s) have been connected properly and protection is provided against electric shock.

Mounting

The unit is available in two versions, DIN Rail/Surface (Wall) Mount, and Rack Mount. The DIN Rail/Surface Mount unit is shipped with the DIN Rail mounting installed. Please refer to Figures 2–1a & 2–1b. For surface or wall mounting, it must be adapted, using the provided mounting hardware. See Figures 2–2a & 2–2b.

Mounting for UL:

For UL listing the unit must be installed in a suitably rated UL Listed fire enclosure

Mounting for CE certification:

The installation must shield the user from high voltage terminals if either of the following options are used:

- 120 Vac/ 240 Vac /125 Vdc power supply
- External FCV supply > 48 Vdc

Note: RS-232, Ethernet and IRIG-B connectors are on the front of units equipped for DIN Rail/Surface mounting. On rack-mounted units, they are on the rear of the unit.

There are no special ventilation requirements for either version. Maximum ambient temperature of +60 ˚C (+140 ˚F) must not be exceeded upon final installation.

Use caution when installing this, or any other type of equipment, into racks or panels. Ensure that all equipment is properly secured using the specified hardware in accordance with the Original Equipment Manufacturer’s (OEM) specifications.

DIN Rail Mounting model SD

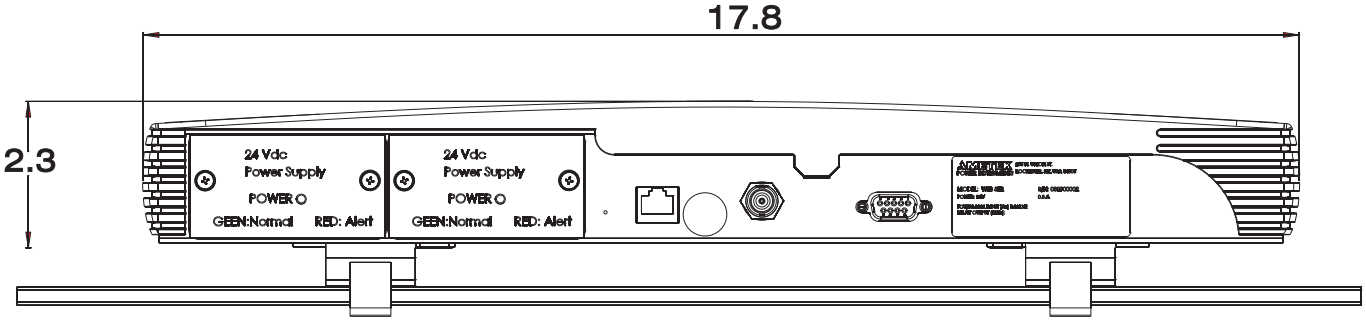


Figure 2–1a DIN Rail Mount, model SD

DIN Rail Mounting models SD1, SD2, and SD3

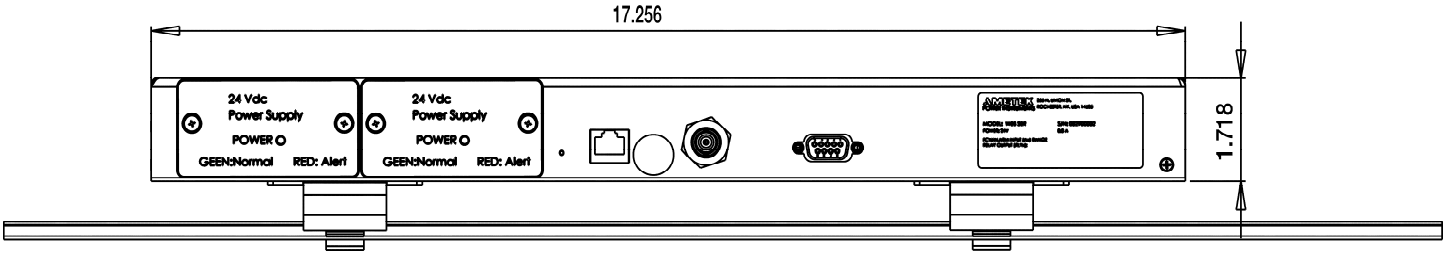


Figure 2–1b DIN Rail Mount, models SD1, SD2, and SD3

Surface Mounting

To convert from DIN rail mount to surface mount:

1. Remove rail mount screws and brackets from bottom of unit.
2. Fasten the wall mounting plates onto the bottom ends of the unit as shown in Fig. 2–2a.
3. Secure the wall plates to the unit with four screws provided for each mounting plate.

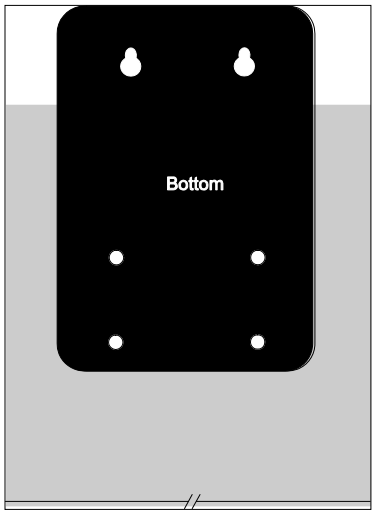


Fig. 2–2a Wall Mount Plate (Bottom View)

Note: Ensure there is proper wall anchoring in the mounting location. After attaching the brackets to the bottom of the unit, hold it in place and mark the holes on the wall, using the brackets as templates. Hang the unit on the wall with two screws in the holes in each wall plate as shown.

Model SD

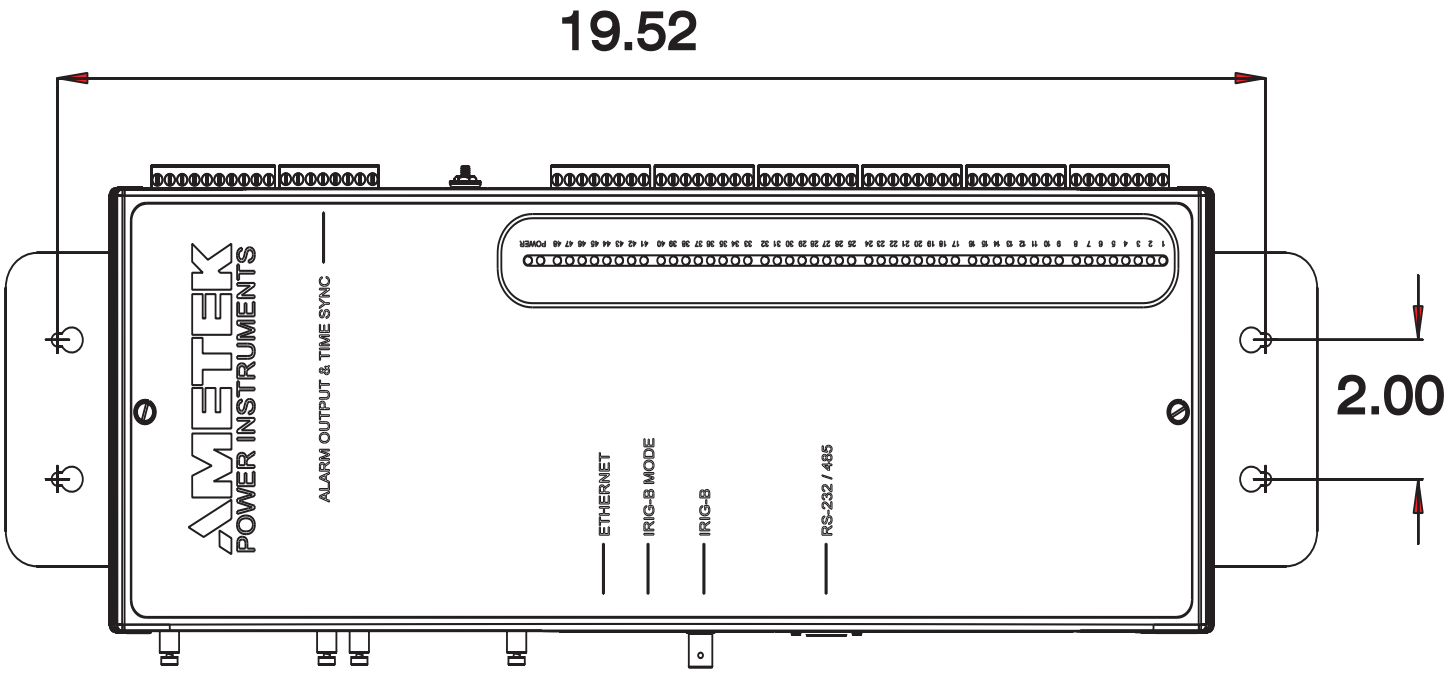


Figure 2-2b, Surface (Wall) Mount, model SD

Model SD1, SD2, and SD3

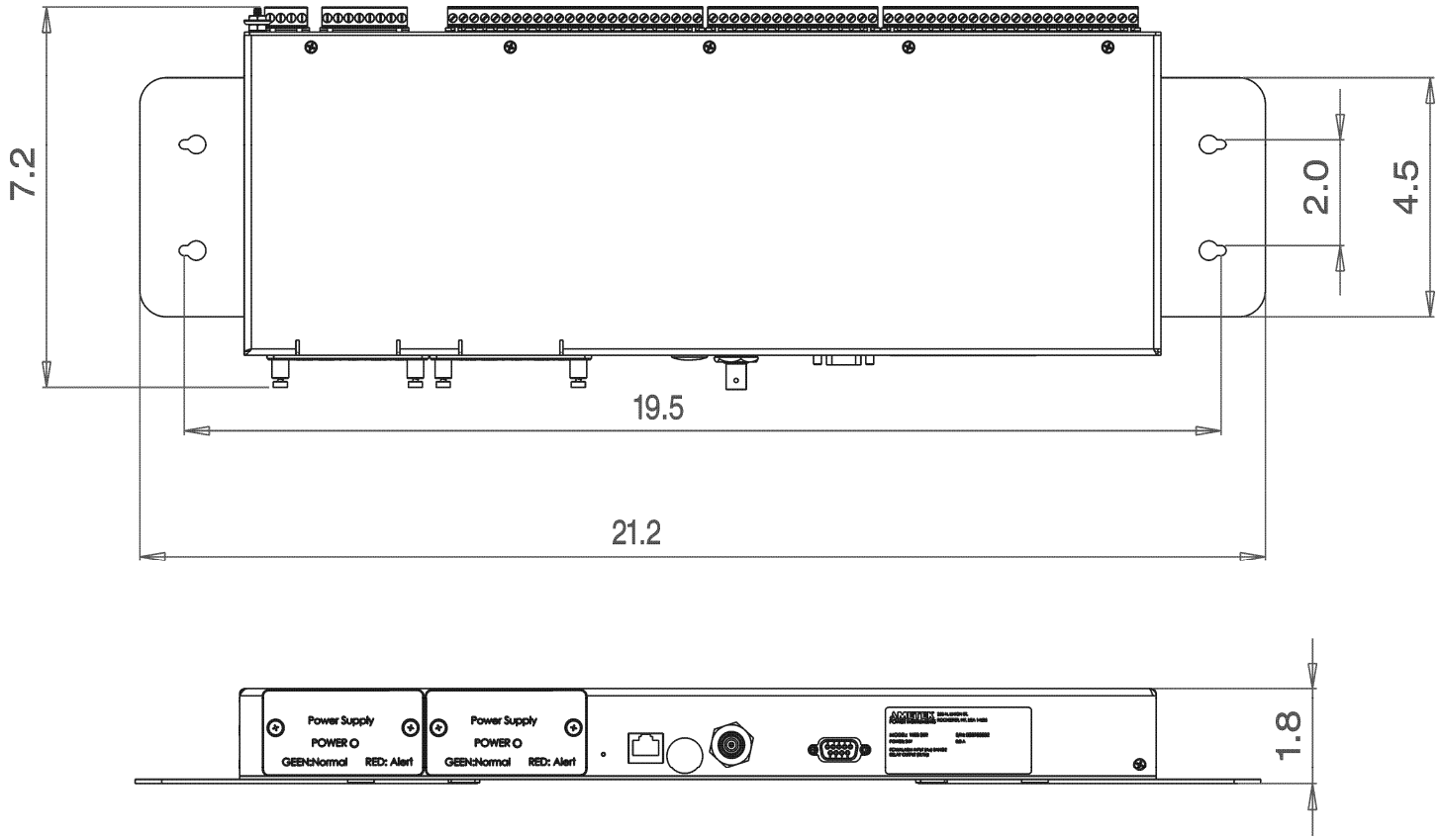


Fig 2–2c, Surface (Wall) Mount, models SD1, SD2, and SD3

Rack Mount model RK

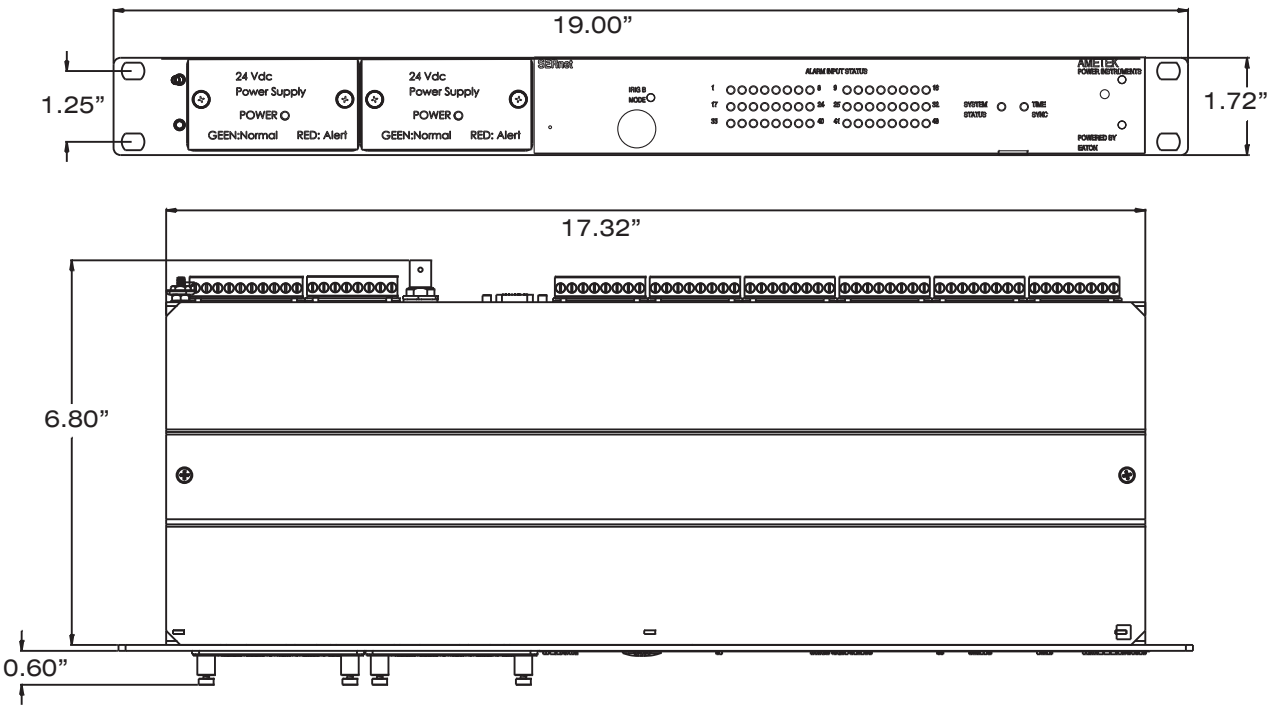


Figure 2–3a, Rack Mount, model RK

Rack Mount models RK1, RK2, and RK3

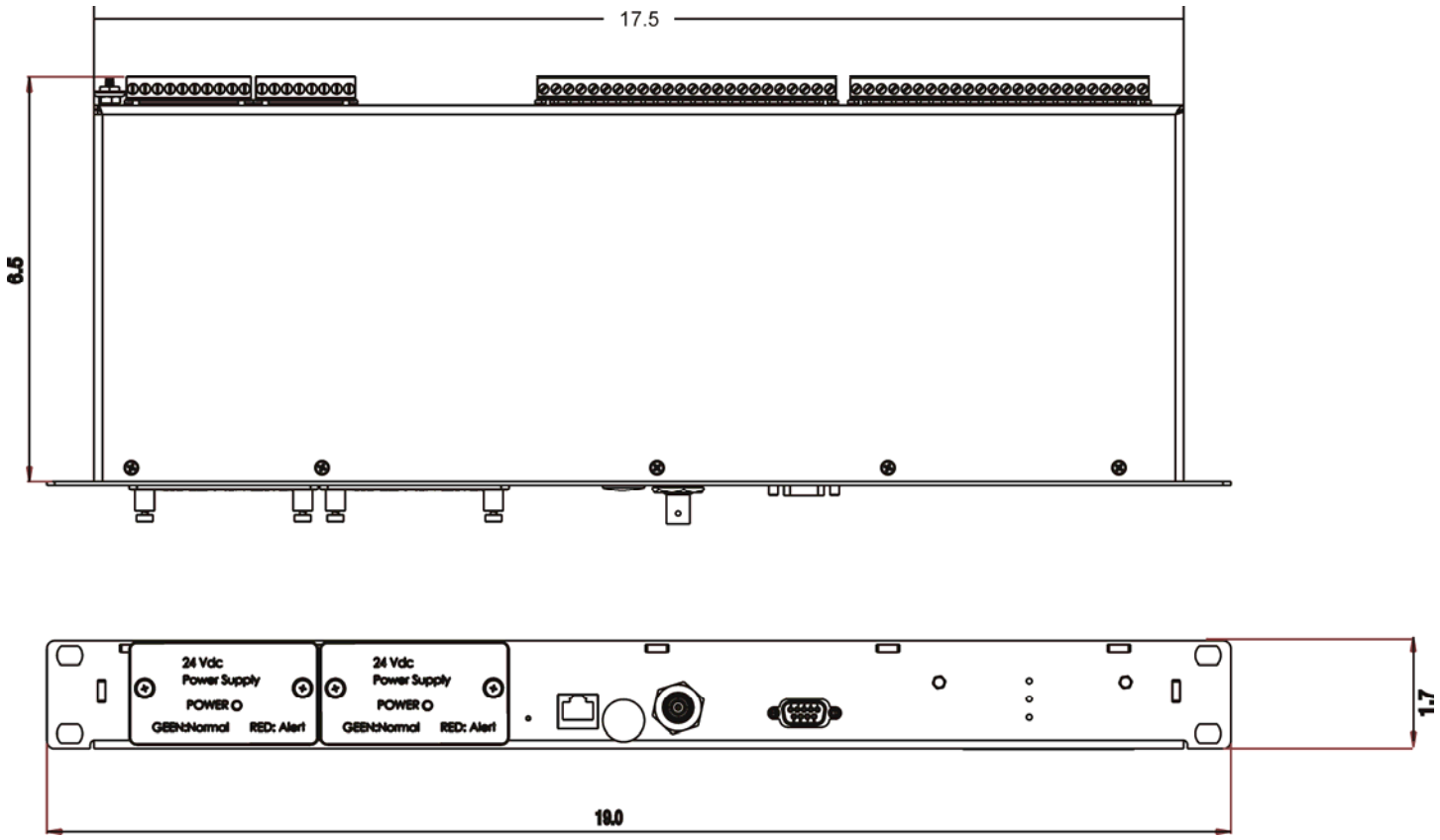


Figure 2–3b, Rack Mount, models RK1, RK2, RK3

ISM Rack Mount

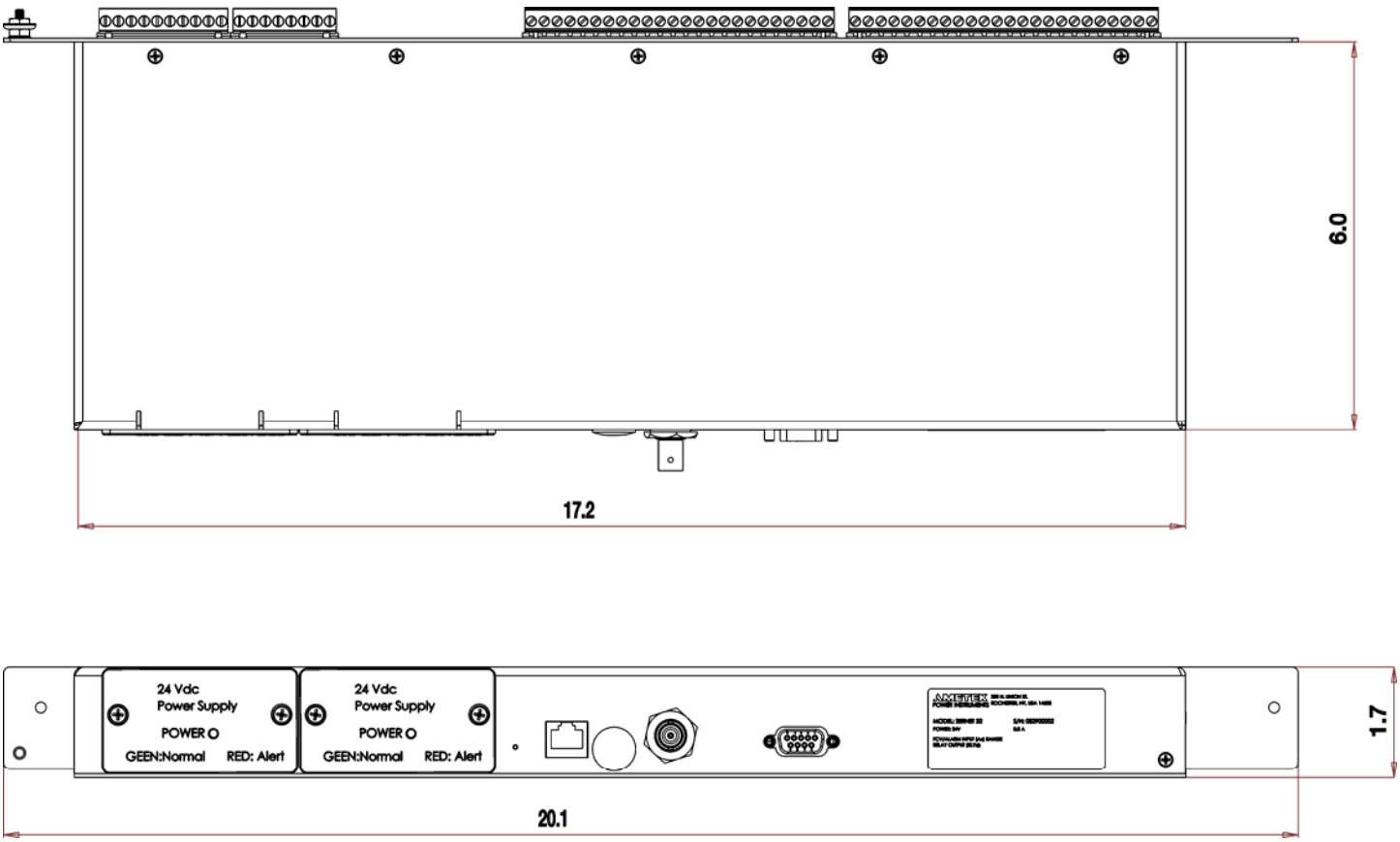


Figure 2–4a, ISM Rack Mount, models ICR1, ICR2, and ICR3

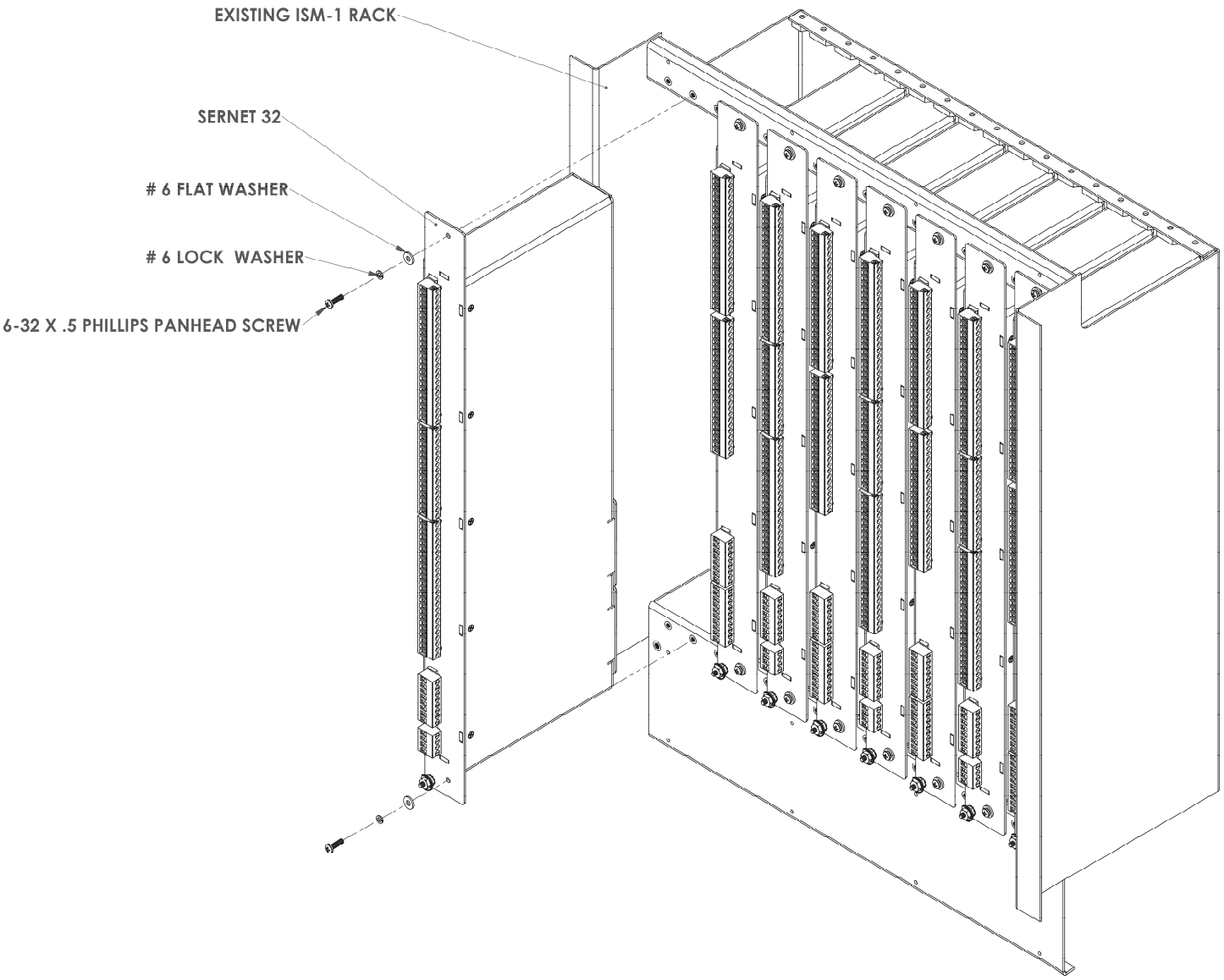


Figure 2–4b, ISM Rack Mount System - Front

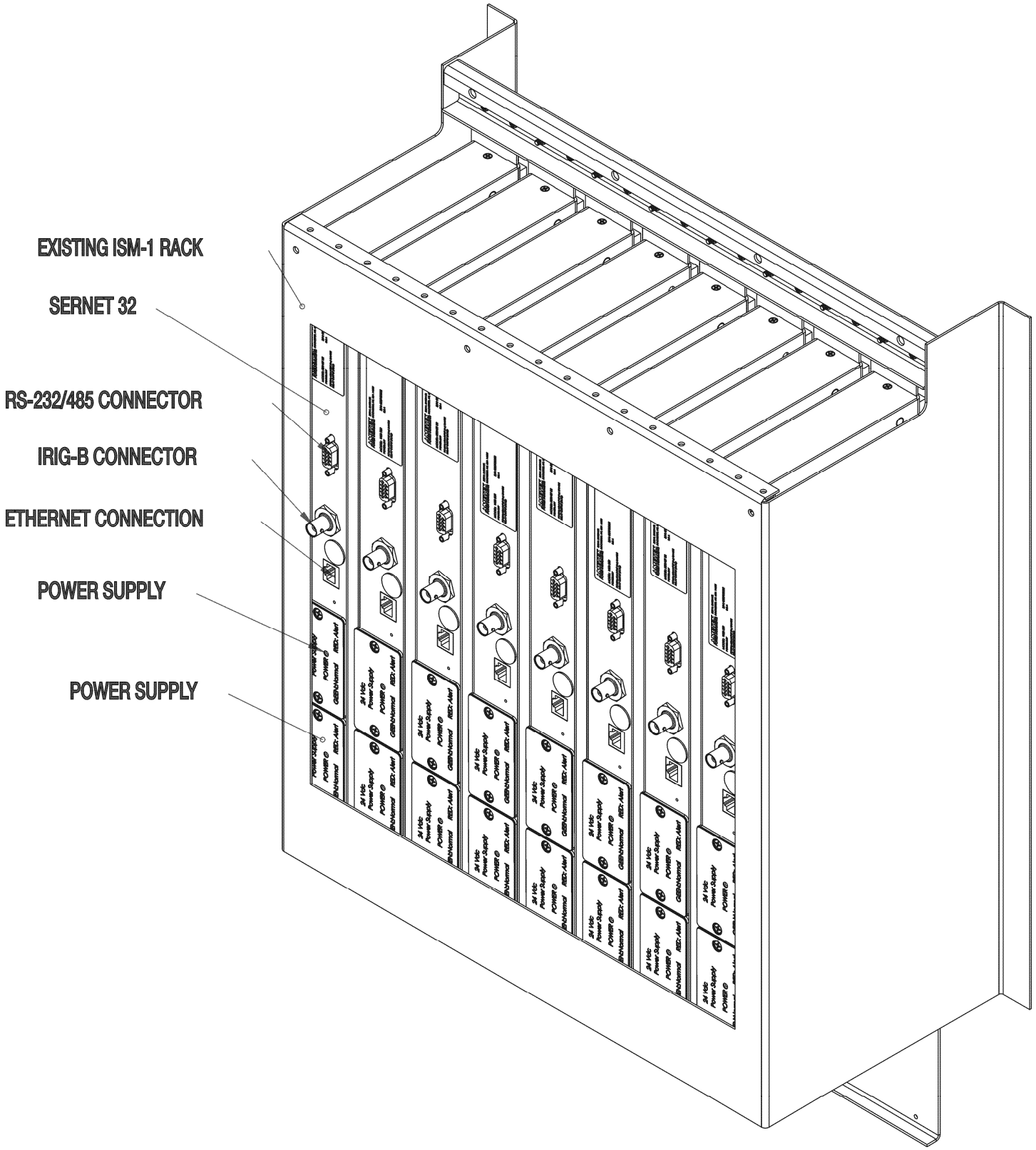


Figure 2–4c, ISM Rack Mount System – Rear

Wiring

Terminal Blocks

Pluggable terminal blocks are used for the power supplies, Field Contact Supply, Field Contact Inputs, and Contact Outputs. The torque rating for the terminal block is as follows:

- Manufacturer PCD (PCD molded in the plastic): 7 Lb.-In.
- Manufacturer Excel (Excel or ECE molded in the plastic): 5 Lb.-In.

The Wire size is 12 – 24 AWG for a single wire. When 2 wires are inserted into a single terminal the wire gauge is limited to 16 AWG

Protective Earth Connection

As shown in the following figures, the Protective Earth Terminal must be connected to protective earth ground. For proper EMC protection, this connection should be made using a minimum ¼" braided conductor or 12 AWG copper wire. For UL listing this connection must be a minimum 12AWG copper wire.

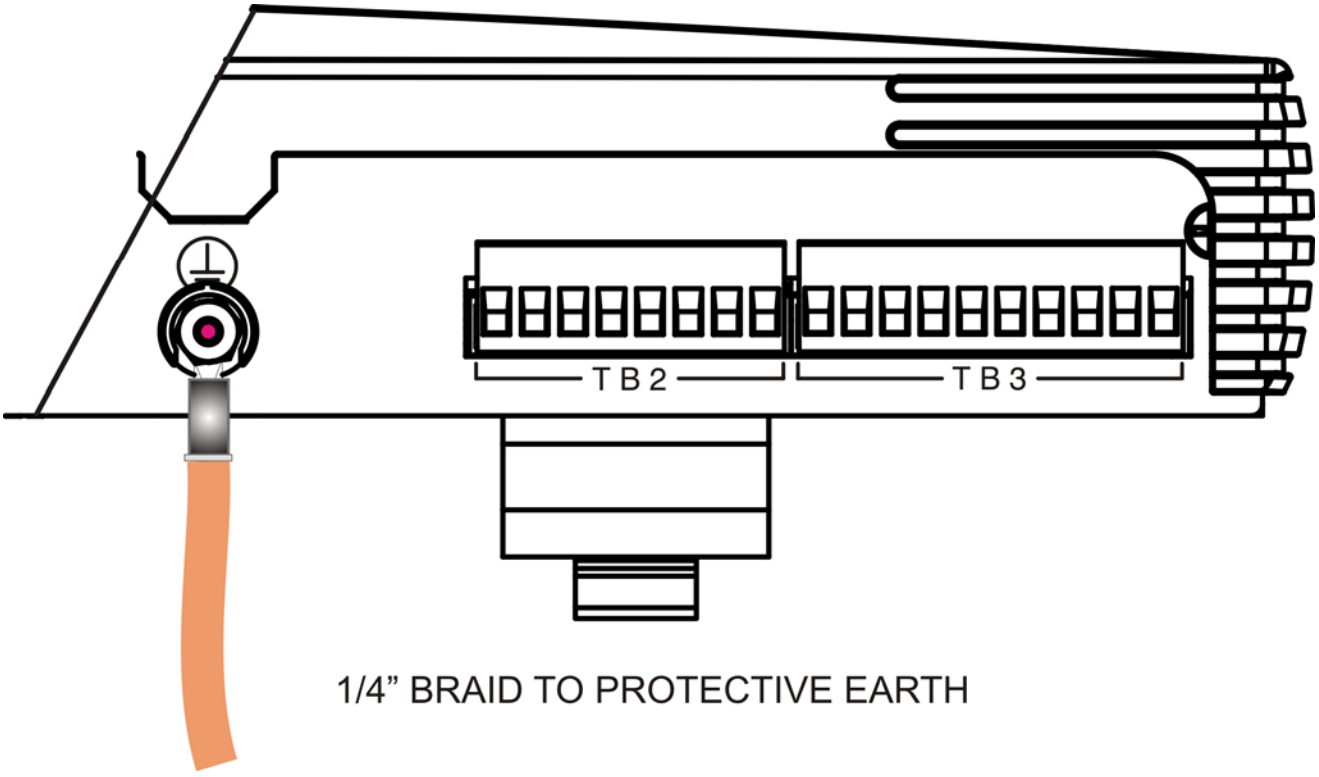


Figure 2–5a, DIN and Surface (Wall) Mount, model SD, Protective Earth Connection.

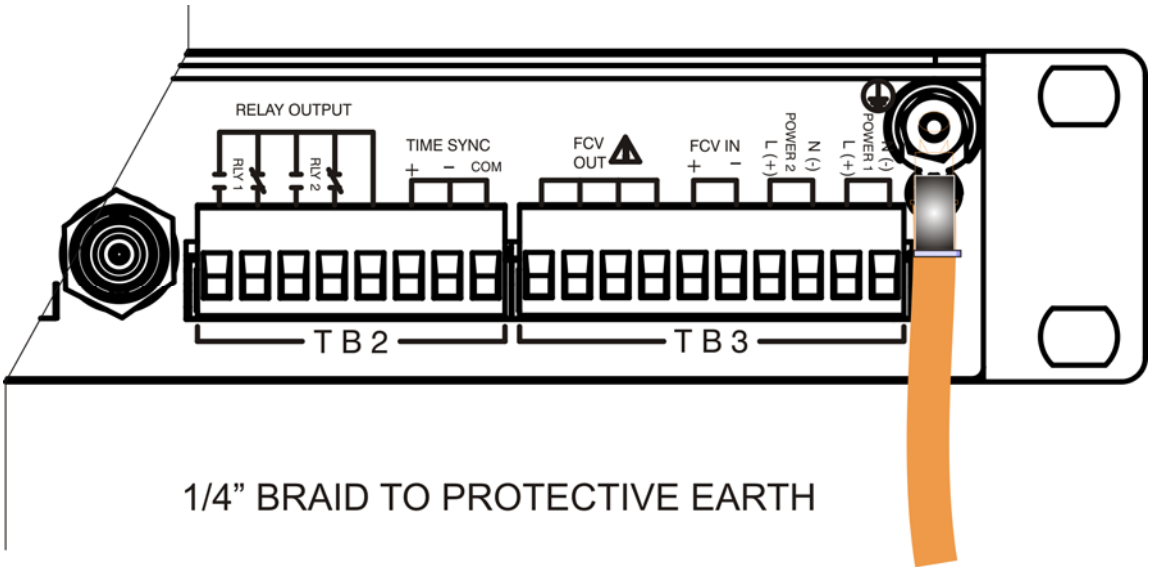


Figure 2–5b, Rack Mount, models RK, RK1, SD1, and ICR1Protective Earth Connection

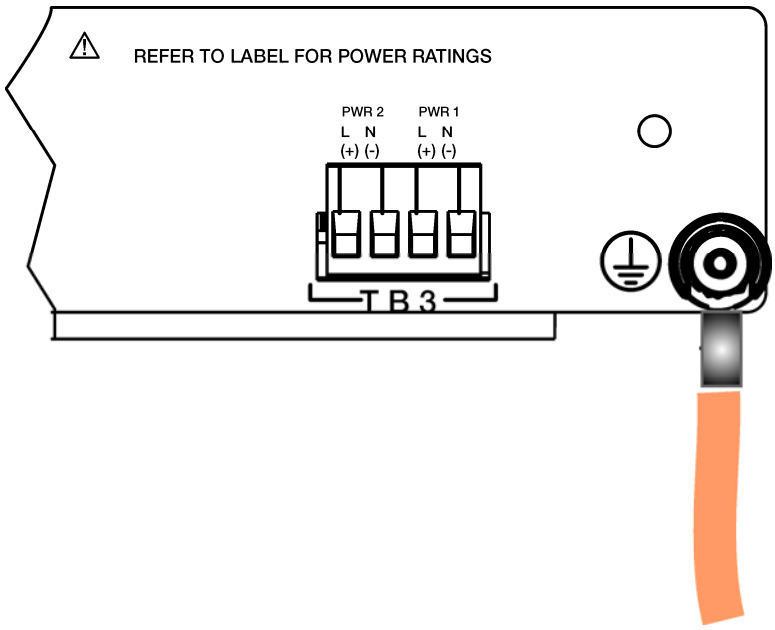


Figure 2–5c, Rack Mount, models RK2, RK3, SD2, SD3, ICR2, and ICR3, Protective Earth Connection

Power Supplies

There are two power supply versions available for SER^{NET}, 120 Vac/240 Vac/125 Vdc, and 24 Vdc.

Either power supply version can be specified for either of the two power supply slots. Refer to the product label, and ensure that the proper voltage is connected to the proper power supply input. The following figures show wiring for a rack-mounted unit, model RK.

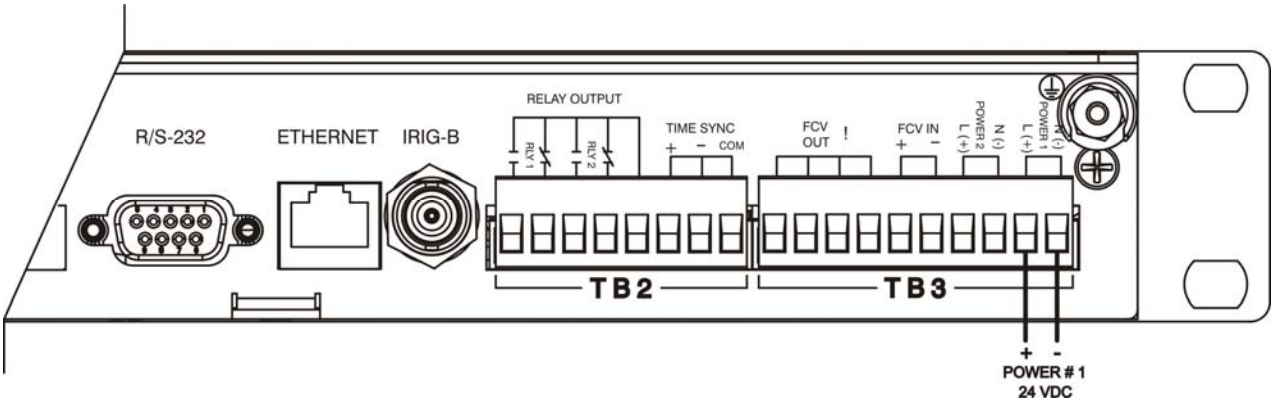


Figure 2–6a, Power Option 1F

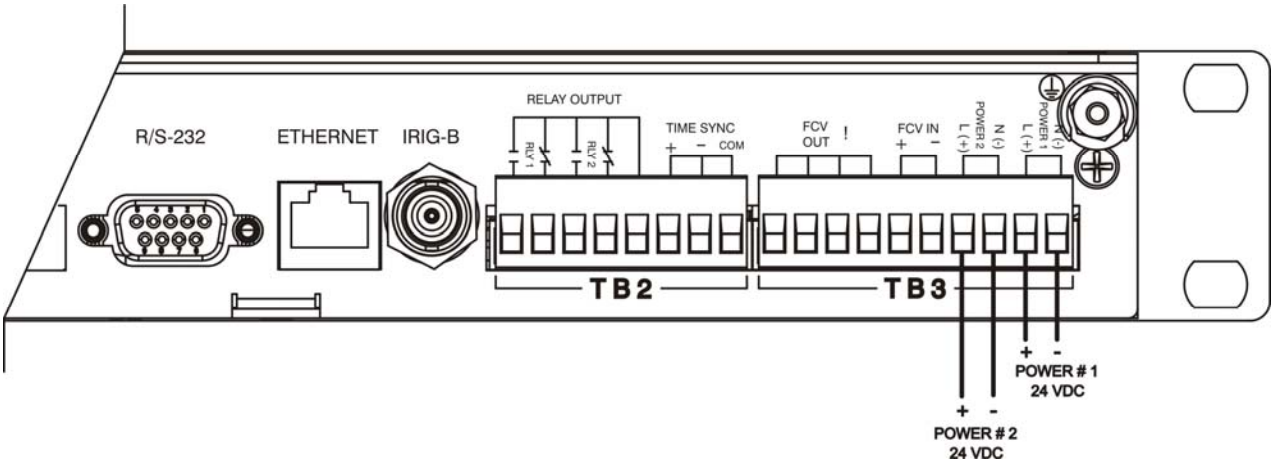


Figure 2–6b, Power Option 2F

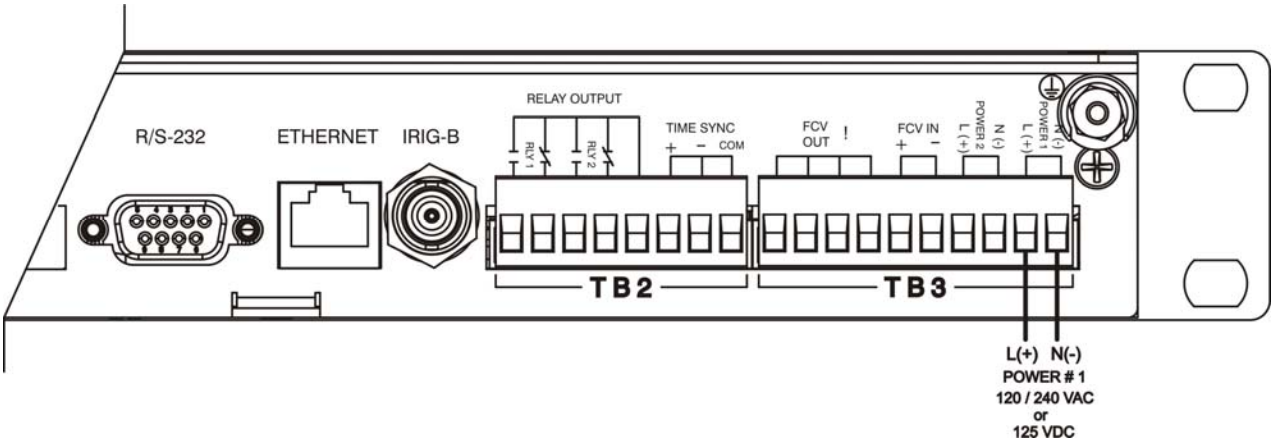


Figure 2–6c, Power Option 1U

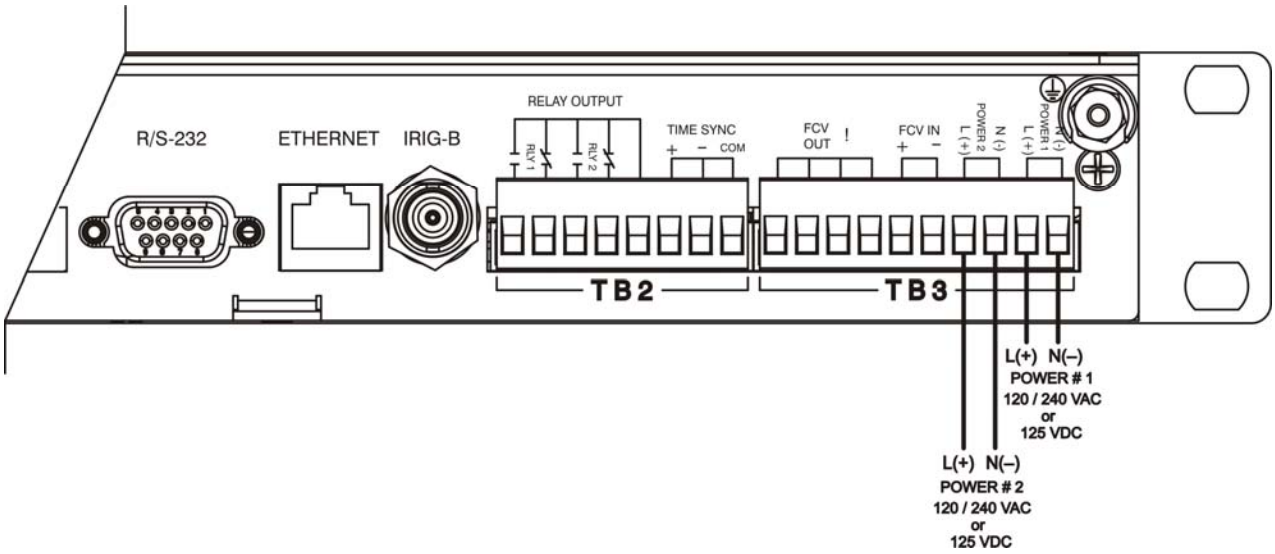


Figure 2–6d, Power Option 2U

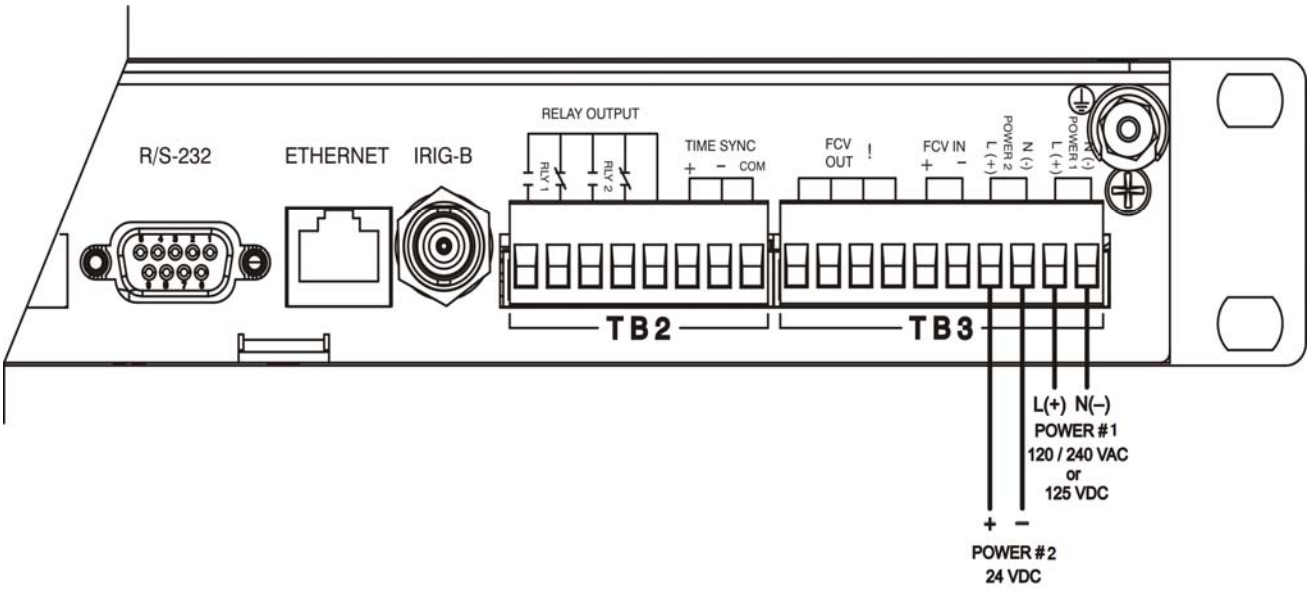


Figure 2–6e, Power Option UF

Field Contact Voltage (FCV)

There are several Field Contact Voltage Options available with the SER^{NET}.

Field Contact Voltage Option	Description	SERNET Models
X	24Vdc internally provided by SER^{NET}	RK, SD, RK1, ICR1, SD1
C	20-150Vdc provided by customer	RK, SD, RK1, ICR1, SD1, RK3, ICR3, SD3
D	125VDC provided by AMETEK supplied External Supply	RK, SD, RK1, ICR1, SD1, RK3, ICR3, SD3
Y	120Vac provided by Customer	RK2, ICR2, SD2

Models SD, RK

This figure shows wiring for a rack-mounted unit, model RK.

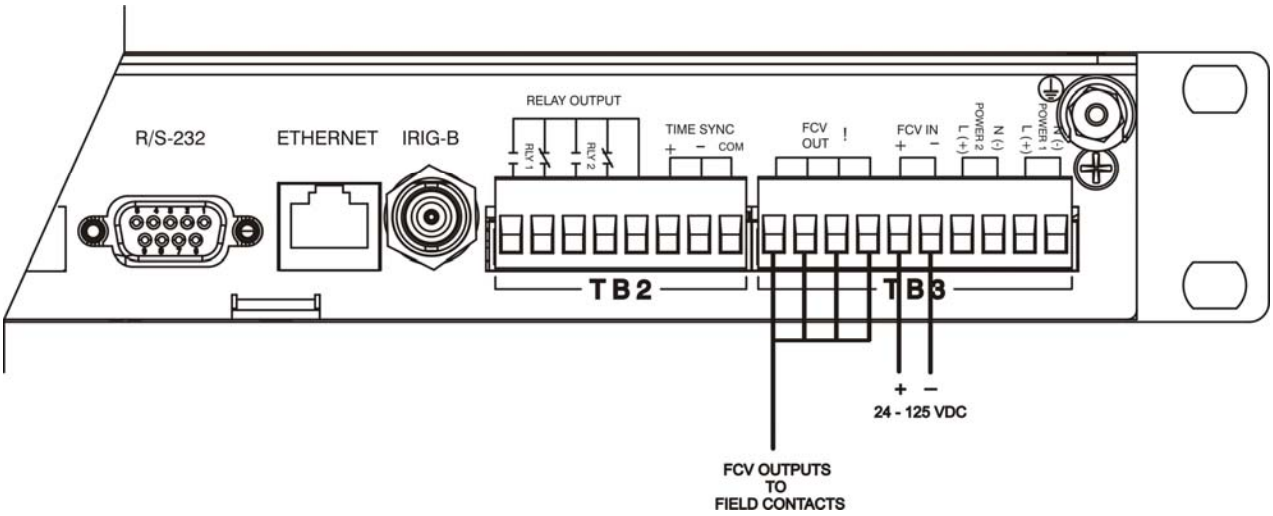


Figure 2–7a, External FCV Input & Output (Options C and D), models SD and RK

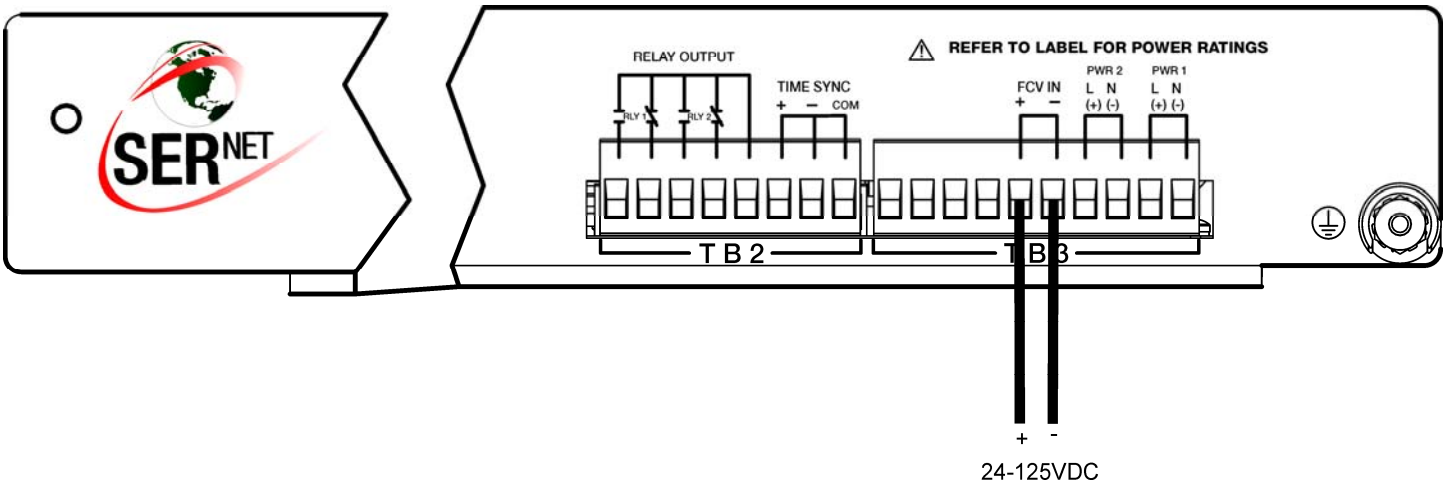


Figure 2-7b, External FCV Input (options C and D), models SD1, RK1, and ICR1

Note: The External FCV is internally routed to the FCV terminals after connecting to FCV IN. Refer to Field Contact Input Wiring, Figure 2-8b

Using External FCV power supplies

External FCV Power Supplies are available for supplying 125VDC to the field contacts. The power supply will accept AC or DC inputs. There are two variations to accommodate a total of 350 or 900 SER^{NET} inputs. A single power supply can provide enough power for several units based on the total number of inputs as shown.

Part Number	Input	Output	# of SER^{NET} Field Contact Inputs
6005-331	100-250VAC/105-300VDC	125 VDC	350
6005-332	90-265VAC/110-350VDC	125 VDC	900

Dimensions: 4.5” W x 2.0” H x 7.8” D

DC Output						AC/DC Input		
+	Not Used	Not Used	**-**	Not used	Not Used	**GND**	**+ (L)**	**- (N)**
1	2	3	4	5	6	7	8	9

Figure 2-7c External FCV Power Supply (6005-331)

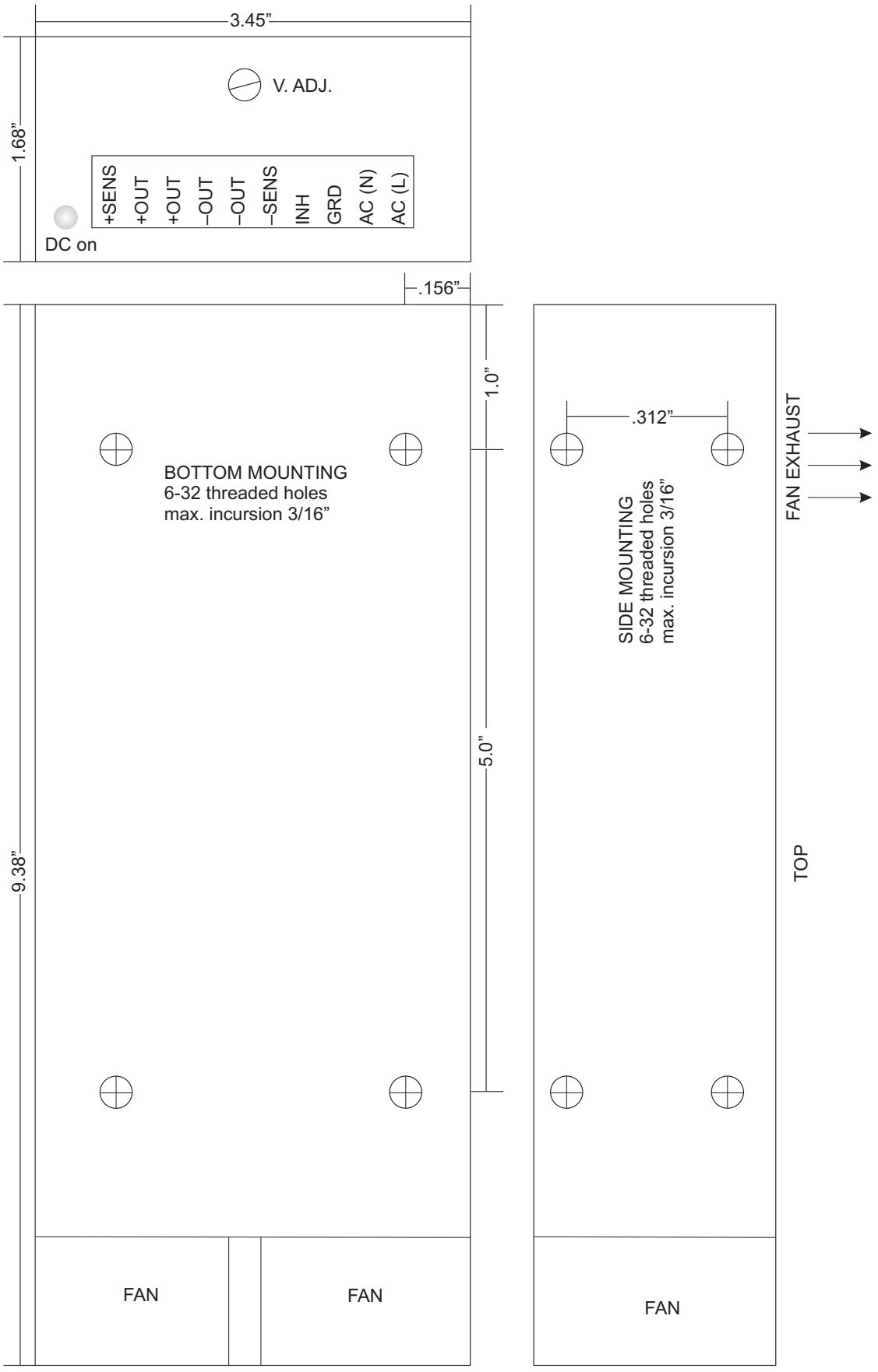


Figure 2-7d External FCV Power Supply (6005-332)

Using existing ISM-1 FCV power supplies

Existing ISM-1 FCV power supplies may be used for the new installation. The FCV voltage can be obtained from the existing 8 position cable, 1064-783, as follows:

Connector position	Wire color	Signal
1	BLK	FCV +
2	RED	FCV +
3	WHT	FCV –
4	GRN	FCV –
5	ORG	Do not use
6	BLU	Do not use
7	BRN	Do not use
8	YEL	Do not use

Select an FCV + wire, either BLK or RED, cut and strip, and connect to the SER^{NET} FCV + input terminal per figure 2-6. Select an FCV – wire, either WHT or GRN, cut and strip, and connect to the SER^{NET} FCV – terminal per figure 2-6a. The remaining ORG, BLU, BRN, and YEL wires are not used and should be terminated appropriately to prevent shorting.

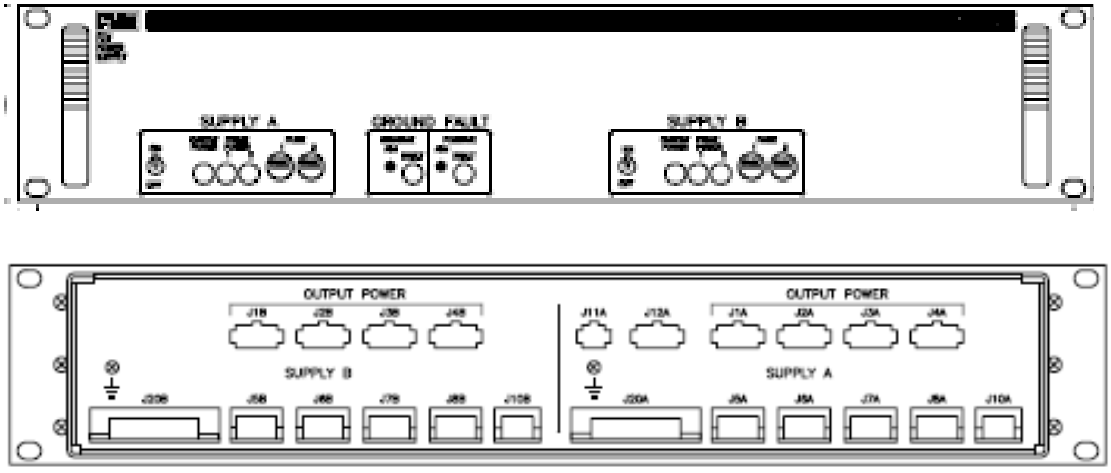


Figure 2-7e ISM-1 FCV Supply

Field Contact Inputs

The unit is factory configured for one of the following options:

Models SD, RK

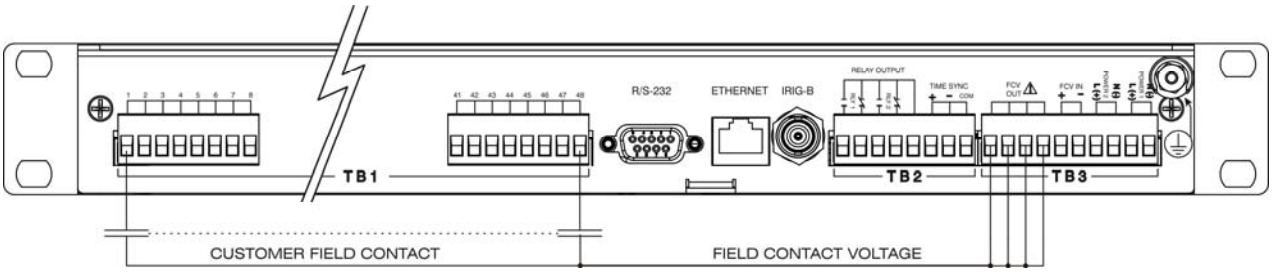


Figure 2–8a, Field Contact Input Connections (FCV options X, C, and D), models SD and RK

Models SD1, RK1, and ICR1

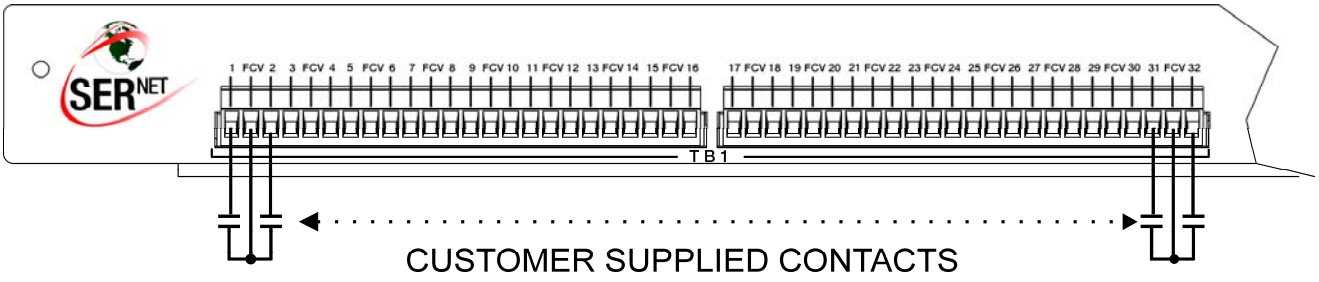


Figure 2–8b, Field Contact Input Connections (FCV options X, C, and D), models SD1, RK1, and ICR1

Models SD2, RK2, and ICR2

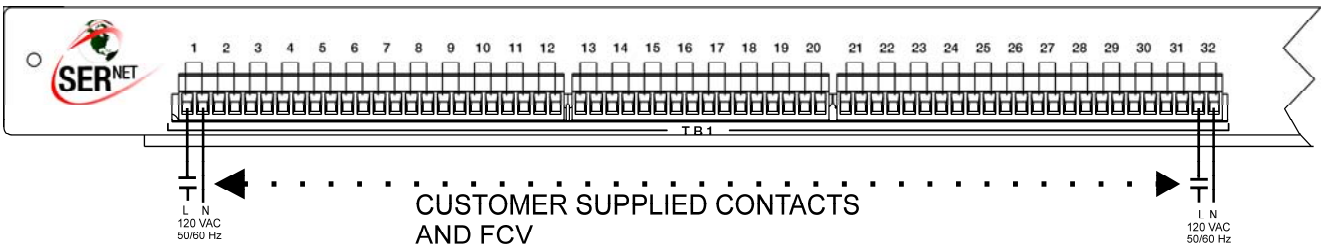


Figure 2–8c, Field Contact Input Connections (FCV option Y), models SD2, RK2, and ICR2

Models SD3, RK3, and ICR3

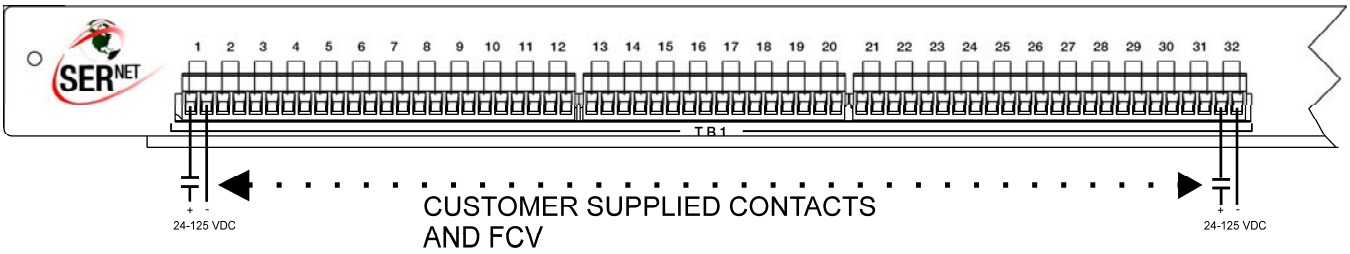


Figure 2–8d, Field Contact Input Connections (FCV options C and D), models SD3, RK3, and ICR3

Relay Outputs

Relay Contact Outputs are configured via the WEB Browser for Alarm, Reflash, Pulsed Alarm or Watchdog. In addition, the coil state can be selected as energized or de-energized in the normal state. Refer to Chapter 3 for more details.

Models RK, SD, RK1, SD1, and ICR1

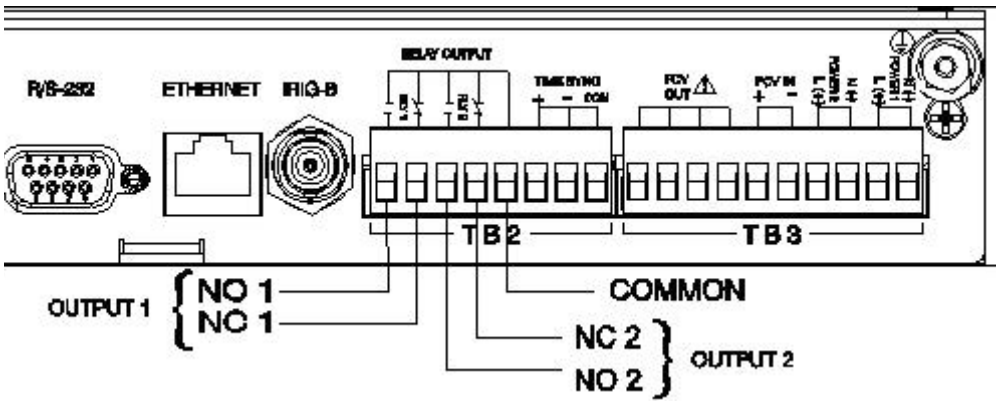


Figure 2–9a, Relay Output Connections, models RK, SD, RK1, SD1, and ICR1. Model RK is shown.

Models RK2, RK3, SD2, SD3, ICR2, and ICR3

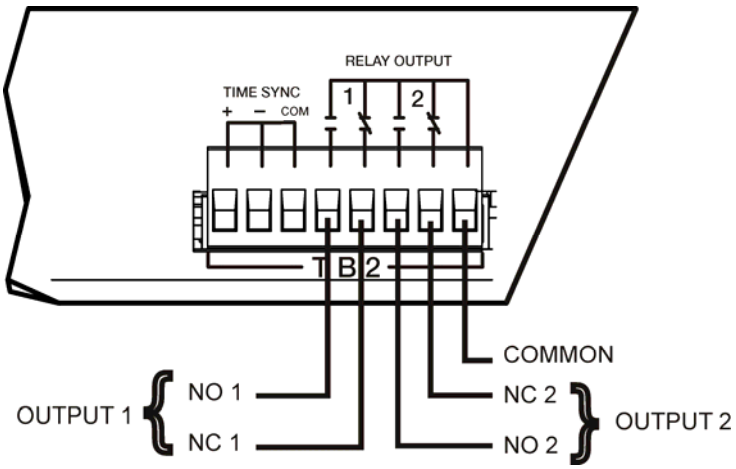


Figure 2–9b, Relay Output Connections, models RK2, RK3, SD2, SD3, ICR2, and ICR3

Serial Port, RS-232 / RS-485

On the *Serial Communications* page of the Web browser, the serial port can be configured for either RS-232 or RS-485 mode. The termination for the RS-485 mode is internal (via checkbox on Serial Communications page).

RS-232 mode

The RS-232 connection is a standard DB-9 female connector. The port can be connected directly to the DB-9 male (AT) connector on a PC. Use a straight cable.

SER^{NET} Signal	SER^{NET} pin	PC pin	PC signal
TX	2	2	RX
RX	3	3	TX
COM	5	5	COM

RS-485 mode

The following are the connections for RS-485 mode

SER^{NET} Signal	SER^{NET} pin
TX/RX +	9
TX/RX –	1
COM	5

Ethernet

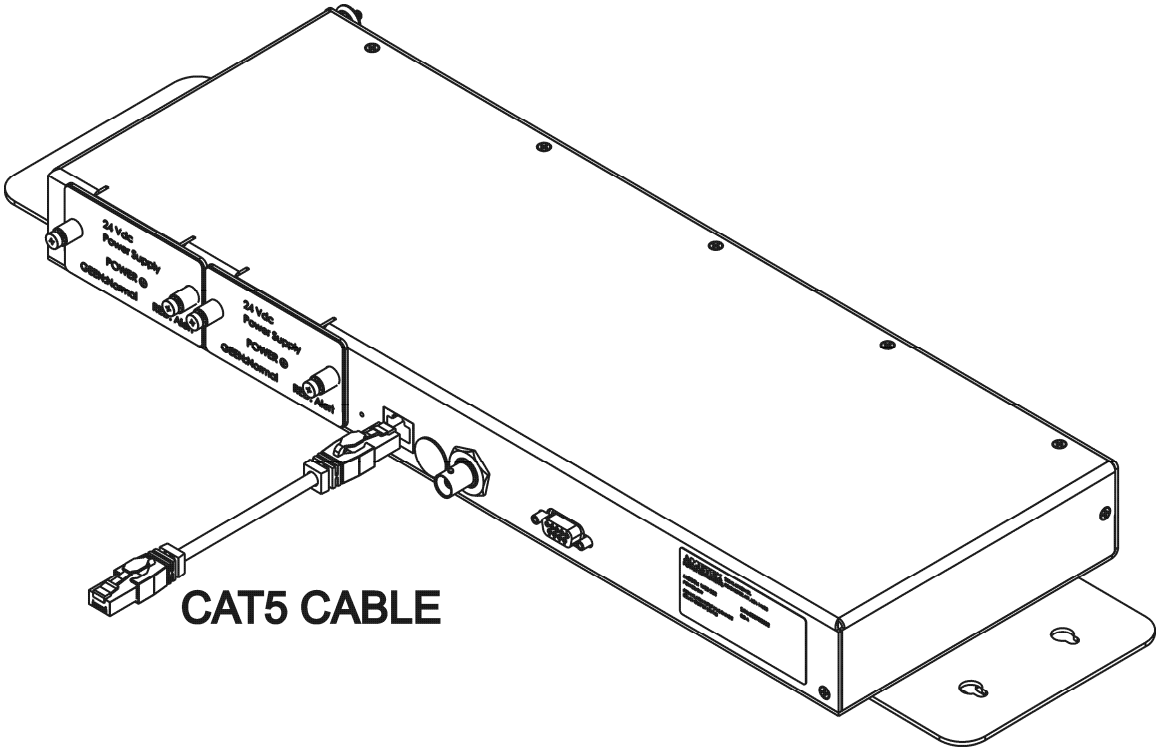


Figure 2–10a, Network Connections

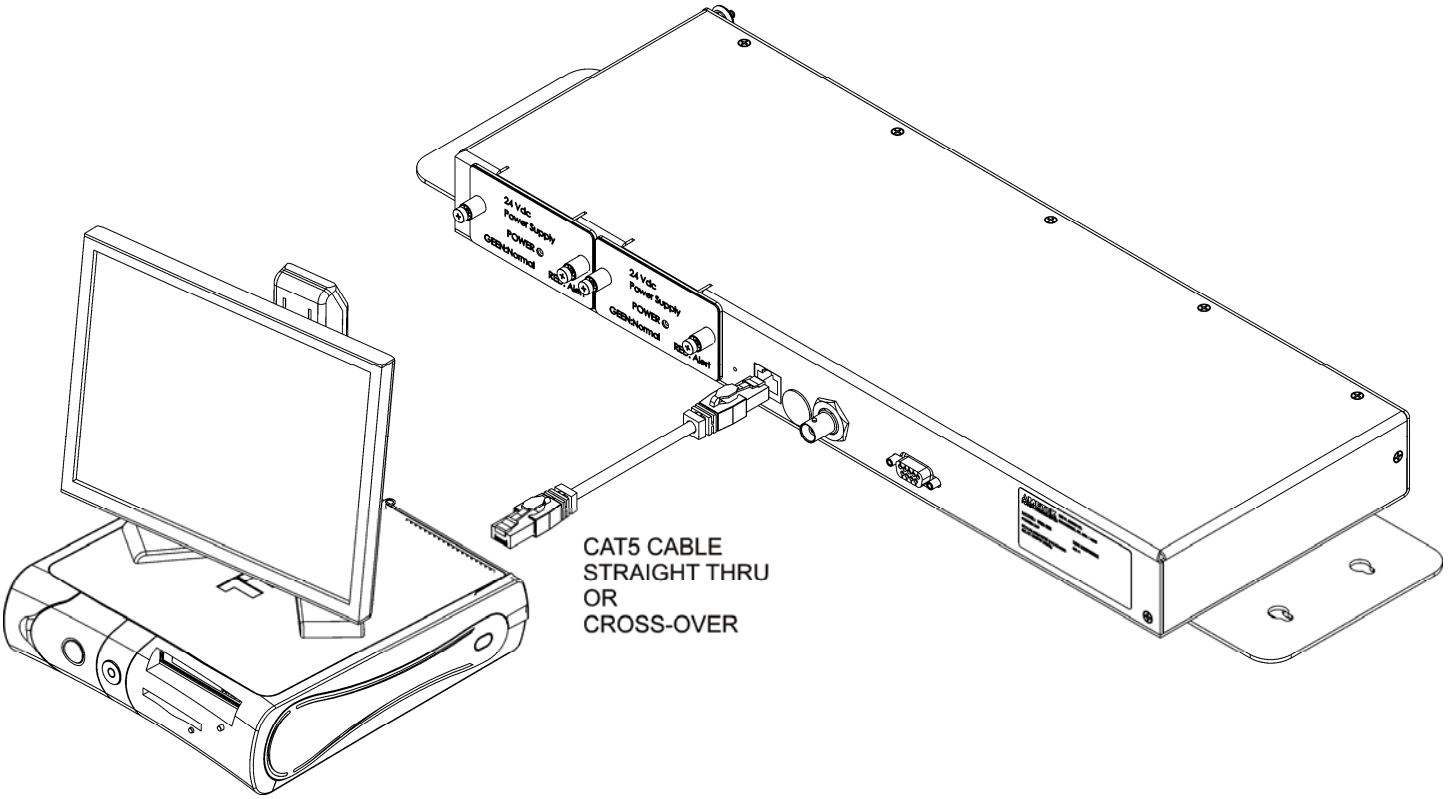


Figure 2–10b, PC Connections

IRIG-B

The IRIG-B signal connects to a standard BNC connector on SER^{NET}. Modulated or Demodulated mode must be selected via DIP switches, which are accessible from the front of the unit. Remove the round plastic cover for access, as shown in the following figure.

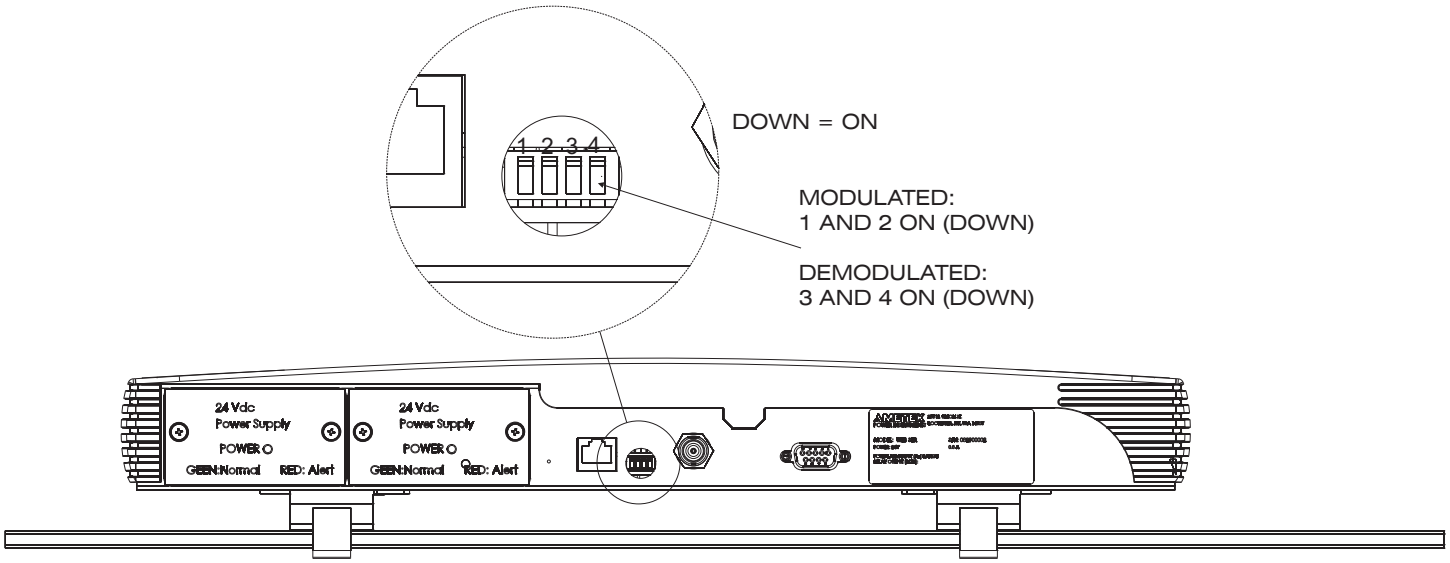


Figure 2–11, IRIG-B Modulated/Demodulated Selection

Selection	1	2	3	4
Modulated	ON	ON	OFF	OFF
Demodulated	OFF	OFF	ON	ON

External Serial Time Sync (unit to unit)

This selection is made on the *Date/Time* page of the Web browser. See Chapter 3.

One SER^{NET} may be designated as a Time Sync Master. All other units connected to the Master must be configured as a Slave.

Models RK, SD, RK1, SD1, and ICR1

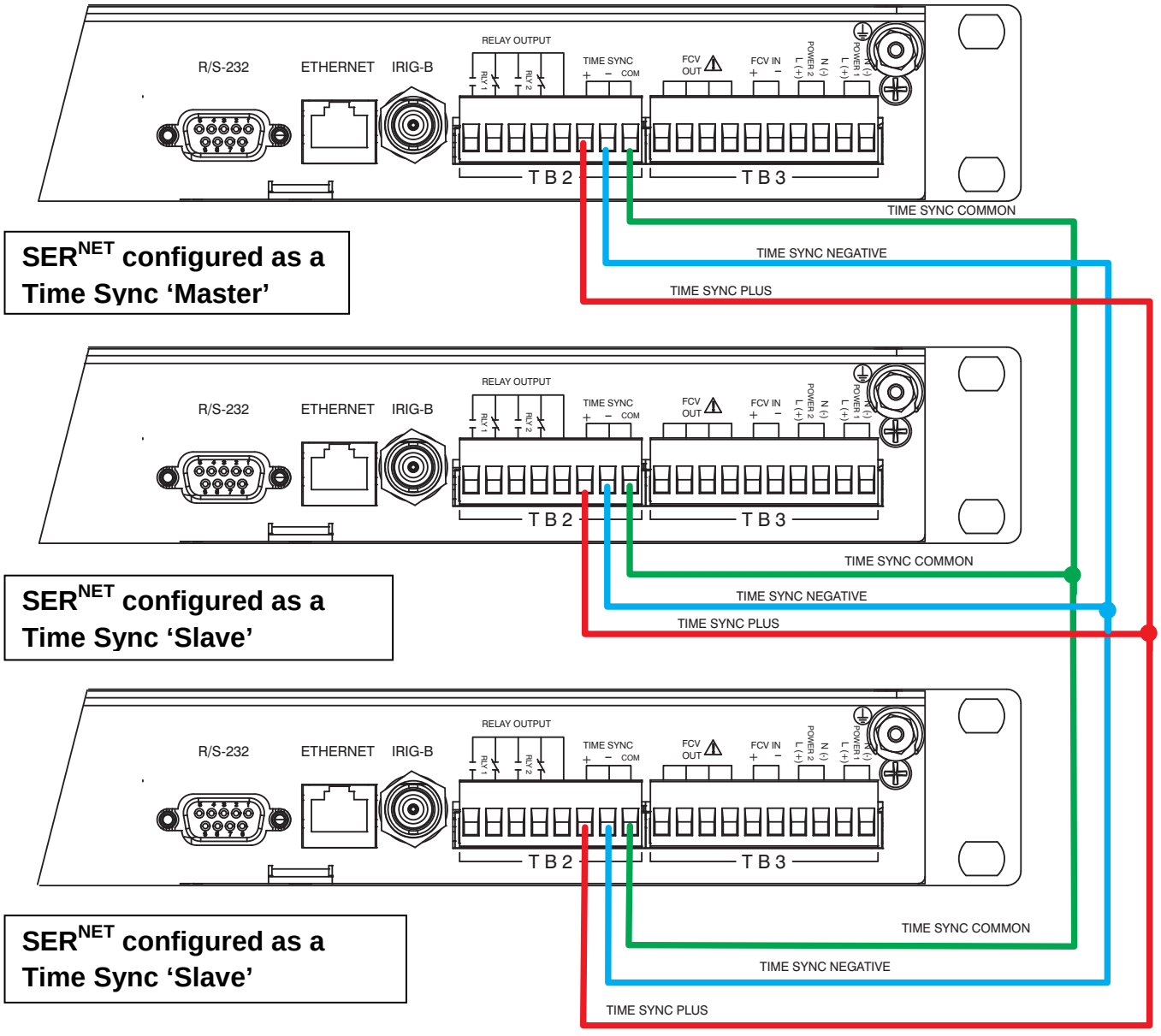


Figure 2–12a, Master/Slave Time Sync, models RK, SD, RK1, SD1, and ICR1

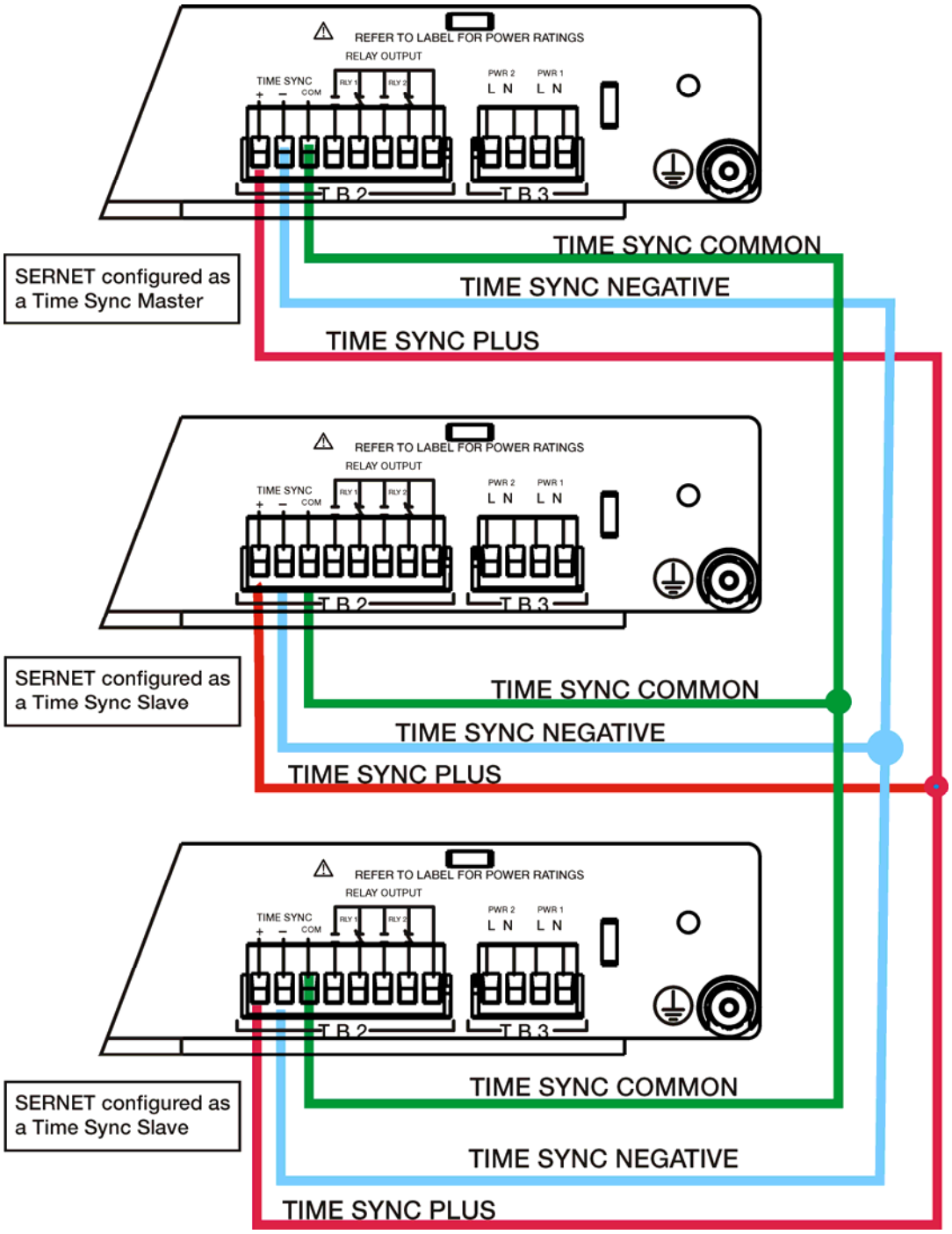


Figure 2–12b, Master/Slave Time Sync, models RK2, RK3, SD2, SD3, ICR2, and ICR3

Chapter 3. SER^{NET} Web Browser Interface

The SER^{NET} has a built-in WEB server that can be used with your Web browser client such as Internet Explorer or Firefox for displaying your alarms and unit configuration. Refer to Appendix F for compatibility requirements and browser configuration.

Launch your browser and type in your unit's IP address. The SER^{NET} is shipped with a default address of: http://192.168.250.100 A User ID/Password dialog box will pop up as shown in Figure 3–1. The SER^{NET} has two levels for access and can be configured as shown, later in this chapter. The default username is: admin with password: admin and user: user. The unit's home page will be displayed where you can view and access all the features of the unit, depending on your user account rights.

Figure 3–1. SER^{NET} Login Dialog Box

Note: Your system or network administrator must set up the user accounts. There are two basic types, Admin and User. An Administrator account has full rights and can change anything. The User account has limited rights and cannot change passwords, apply or discard changes. Some action buttons will be grayed out under a User account.

WEB Browser Alarm Display

The SER^{NET} can display the alarms as they occur using a graphical 'Annunciator style' display on the Home page, Active Alarm Display showing all inputs that are in the alarm state with time stamps and an Event Display that shows current alarms and historical alarms with time stamps for analysis and download.

SER^{NET} Home Page/Digital Alarm Home Page

Figure 3–2a shows the home page and/or Digital Alarm Home Page with administrator logged in. The top bar of the home page displays the current date/time (in UTC and local time), and latest alarm that is *not* acknowledged. The check box – *Enable 30 second auto-refresh*, when checked, will refresh the page every 30 seconds.

The main page has a graphic display of the alarms and several editable fields that identify the unit's Station ID and Device ID. The graphic display of the SER^{NET} is provided with alarms shown in any selectable color with their alarm legend. Inputs in their normal state will be shown with a user selected background and their normal legend. When the alarm clears, the display automatically refreshes itself to the normal state. Alarm inputs that have been disabled will have a user selectable color background to highlight the disabled state. Customizing the color schemes is done through the 'Color Selection' menu described later in the manual. The configuration below has new alarms shown in red background, acknowledged alarms in green, disabled alarms in yellow and normal inputs in a clear background.

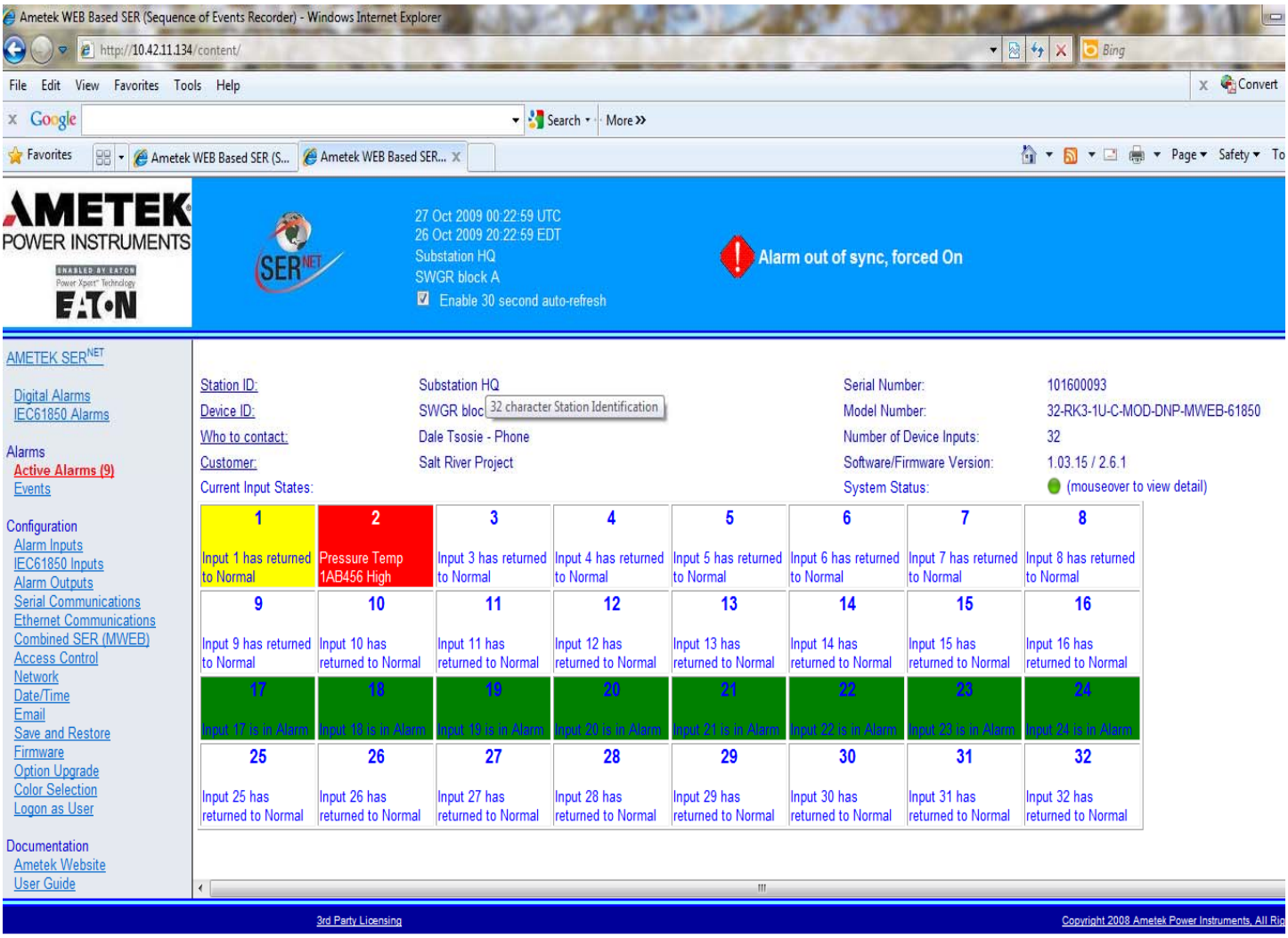


Figure 3–2a. SER^{NET} Home Page

The home page also provides real time status of various diagnostics by moving the mouse over the green (red) indicator shown in the upper right hand side of Figure 3-2a. This indicator mimics the System Status LED on the front of the unit. Green color indicates all items are normal and red indicates a failure. Figure 3–2b shows the pop-up.

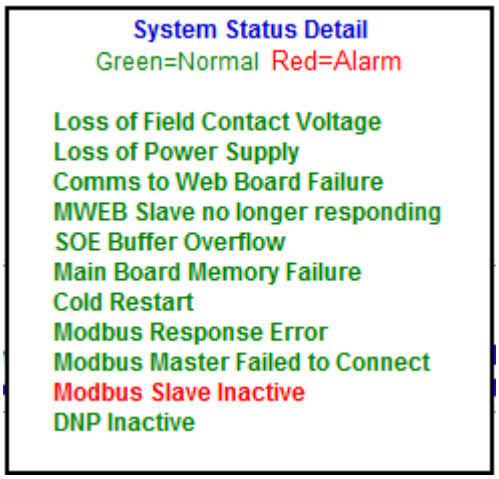


Figure 3–2b. System Status Detail

The diagnostics include:

- Loss of Field Contact Voltage
  The Field Contact Voltage (FCV) internal supply has failed or the external field contact voltage has not been detected on the FCV terminals.
- Loss of Power Supply
  One of the internal power supplies is not operating.
- Comms to WEB Board failure
  There is an issue with the internal communications of the unit.
- MWEB Slave no longer responding
  In systems configured for MWEB, one of the slave units is no longer communicating to the Master.
- SOE Buffer overflow
  The number of alarms received exceeded the capability of the unit. 80 events/sec x 35 inputs per unit for several minutes
- Main Board memory failure
  There is an internal failure with the system memory
- Cold Restart
  The unit has performed a cold restart either manually or after a new firmware upgrade
- Modbus Response Error
  The Modbus device connected to the SER^{NET} has not responded to a poll request or it has received a request that is not supported.

- Modbus Master Failed to Connect
  The SER^{NET} Modbus Master did not receive a response from the Modbus Slave device
- Modbus Slave inactive
  The SER^{NET} Modbus slave has not received a request from a Modbus master device
- DNP inactive
  The SER^{NET} DNP slave has not received a request from a DNP master device

Systems with MWEB Option (Combined Master)

The Combined SER MWEB option (firmware 1.01+) enables a single SER^{NET} master to manage and collect alarms from up to 24 slaves in one browser window. For combined systems where a Master Unit collects alarms from multiple Slave units (MWEB option), the top header of the Master Unit will indicate 'Combined SER Master' in place of the latest Alarm as shown in Figure 3-2c

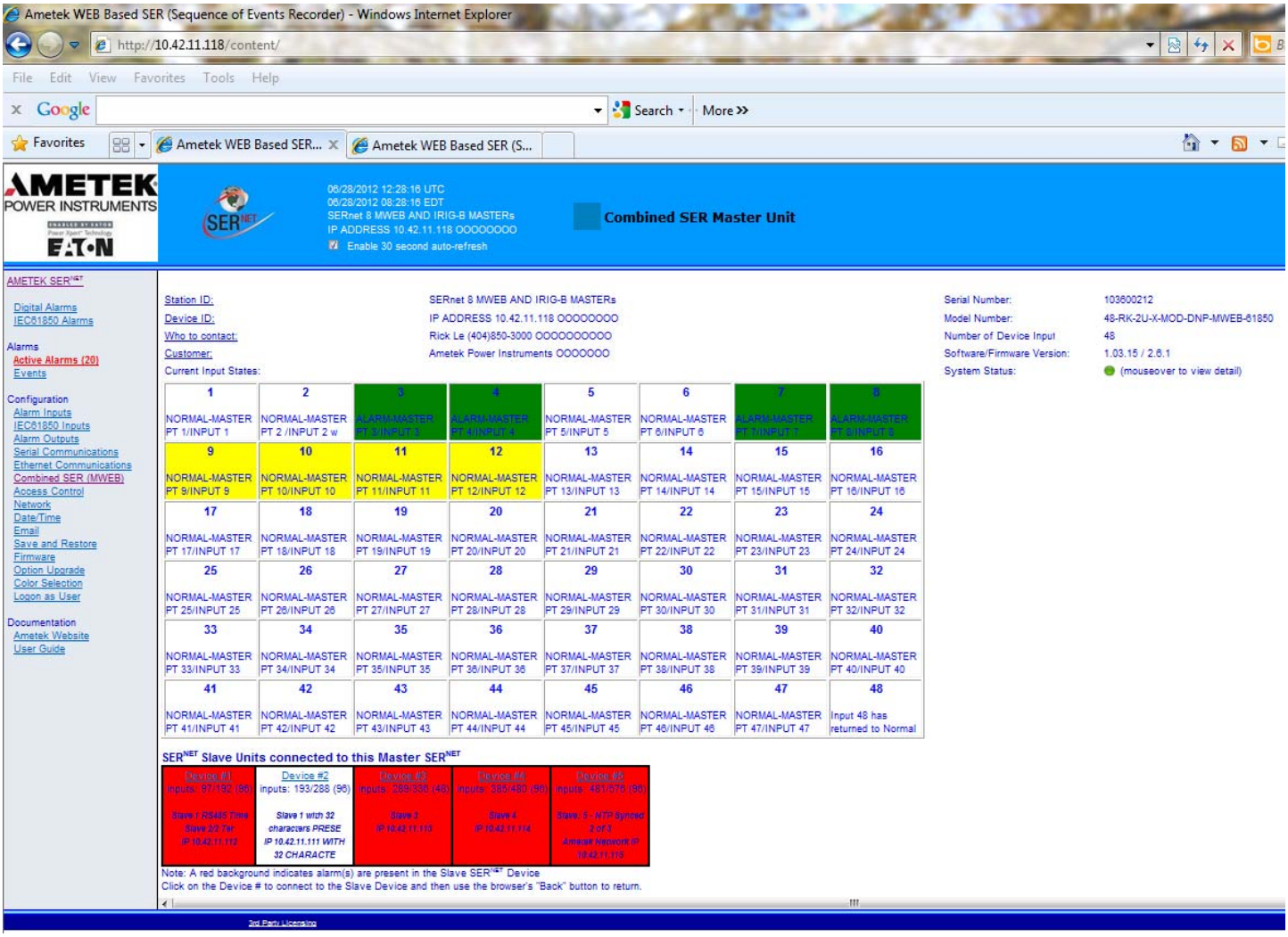


Figure 3–2c. SER^{NET} Home page Set-up as MWeb Master

The Master SER^{NET} equipped with the MWEB option will include a graphic showing every Slave SER^{NET} unit connected. As shown in figure 3-2d, the graphic will include the Slave Station ID, Device ID and Input numbers assigned to the slave unit. When an alarm is present on that slave unit, it will have a red backfill.

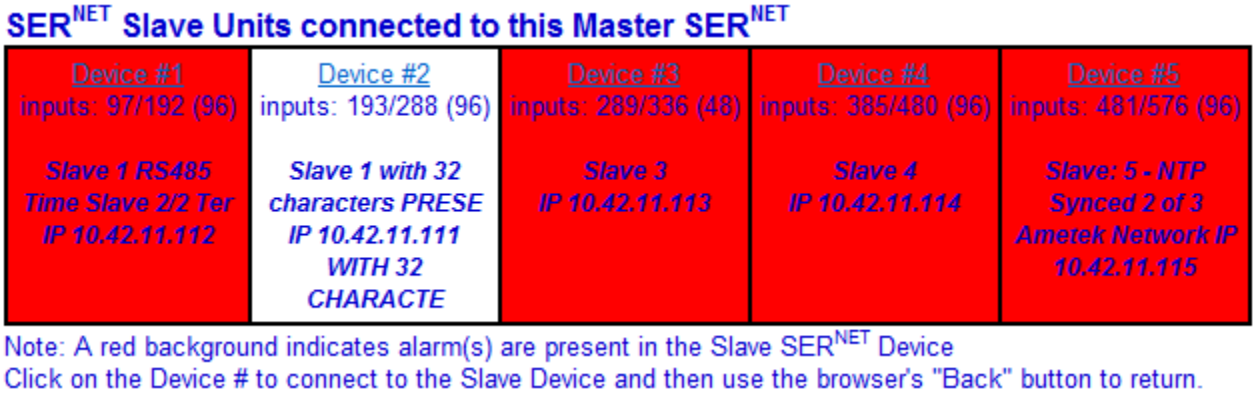


Figure 3–2d. SER^{NET} Slaves (on Combined SER MWEB Page)

Systems with IEC61850 Option – IEC61850 Alarms Home Page

If the unit is equipped with the IEC 61850 option, the IEC 61850 alarms received by the SER^{NET} can be displayed on the WEB Browser Graphic Screen. Figure 3–2e shows the IEC61850 Alarm home page with administrator logged in. The top bar of the IEC61850 home page displays the current date/time (in UTC and local time), and latest alarm that is *not* acknowledged. The check box – *Enable 30 second auto-refresh*, when checked, will refresh the page every 30 seconds.

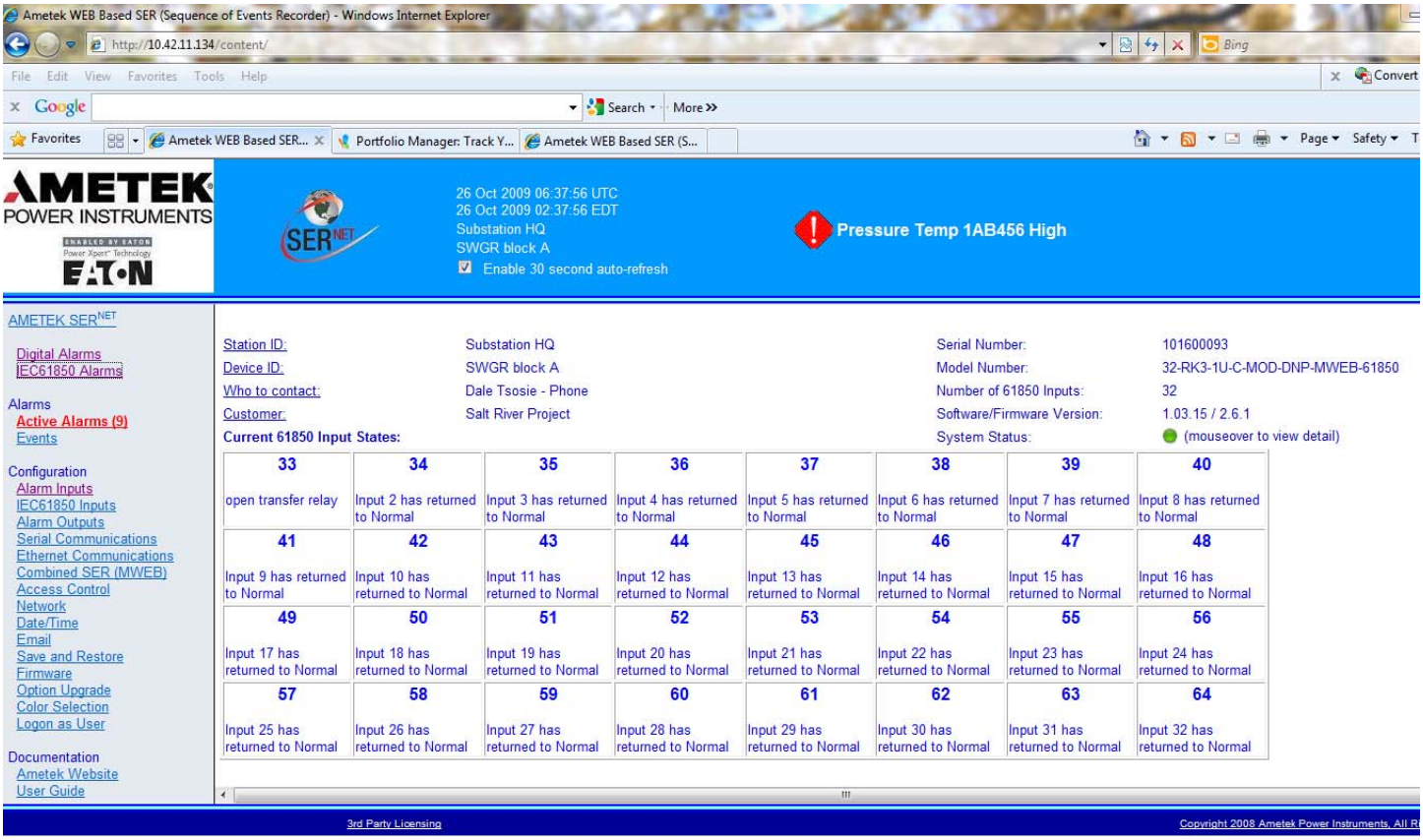


Figure 3–2e. SER^{NET} IEC61850 Alarm Page

The IEC61850 home page has a graphic display of the alarms and several editable fields that identify the unit's Station ID and Device ID. The IEC61850 numbering sequence would begin after the last digital input number used on the Digital Alarms home page.

Example: 1-32 on SER^{NET} Digital Alarms home page, 33-64 on the SER^{NET} IEC61850 Alarms home page.

The graphic display of the SER^{NET} IEC61850 alarms home page will follow the same user selected coloring sequence implemented on the Digital Alarm home page.

Home Page Editable Fields

In this section, please refer to the links directly below the top bar. The items on the right, *Serial and Model Numbers*, *Number of Device Inputs* and *Software/Firmware Version*, are configured at the factory.

Links that you can edit are underlined. When you click on a link in this section, a small dialog box will appear where you can enter the appropriate information (see Fig. 3–3). After typing in a name, for instance, you simply click the save button. All editable fields, i.e. Station ID, may contain up to 32 alphanumeric characters.

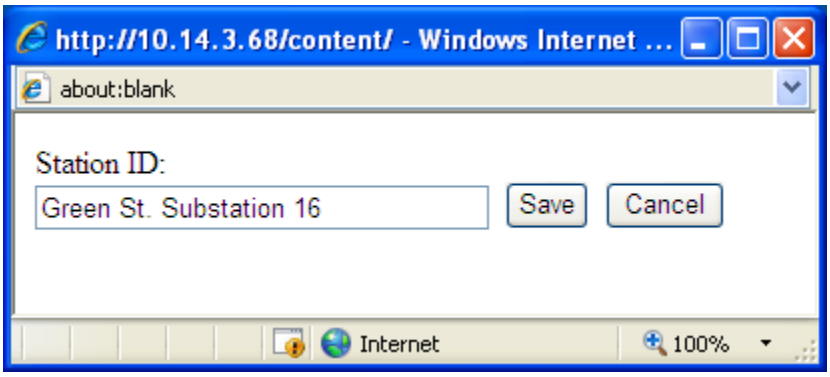


Figure 3–3. Pop-up Dialog Box

Station ID

Click this link to enter a specific location name for the unit. i.e. Green St. Substation 16. This name will be reported in the Active Alarms and Events list, event download, ASCII output and printouts.

Device ID

This name is more specific, i.e. to identify a single unit in a substation containing many units. It should be used to identify a SER^{NET} unit or group of alarms connected to the unit. i.e. SER^{NET} Device 1 or Breaker XYZ. The device ID will be reported in the Alarms and Events list, event download, ASCII output and printouts.

Who to Contact

This field is used to identify a contact such as in case of emergency.

Customer

Here is where you enter the customer's name.

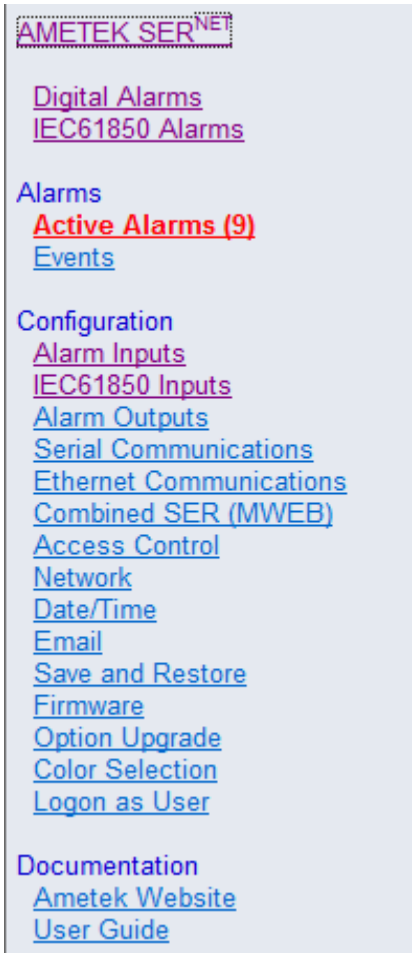


Figure 3–4. SERNET Navigation Sidebar

WEB Browser Navigation

The side-bar on the home page contains links to all of the pages for unit access and configuration.
The AMETEK SER^{NET} link on the top always redirects you to the Home Page shown in Figure 3-2a, similarly to when Refresh is performed on the Browser.

The side-bar is separated into two Categories: Alarms and Configuration. The links under 'Alarms' allow you to view active or historical alarms. The links under 'Configuration' are used for configuring the SER^{NET} unit.

Active Alarms Page

The Active Alarm screen is used as a 'heads-up display' for identifying all inputs that are currently in the alarm state. This will include IEC61850 points if the SER^{NET} has that feature enabled. When the SER^{NET} is equipped and set-up with the MWEB option, the Master SER^{NET} will display alarms from itself as well as every slave SER^{NET} connected to it, in chronological order, The Active Alarm screen provides the ability to latch alarms until acknowledged and includes various user selectable color coding features to distinguish new alarms. Customizing the color schemes is done through the 'Color Selection' menu described later in the manual.

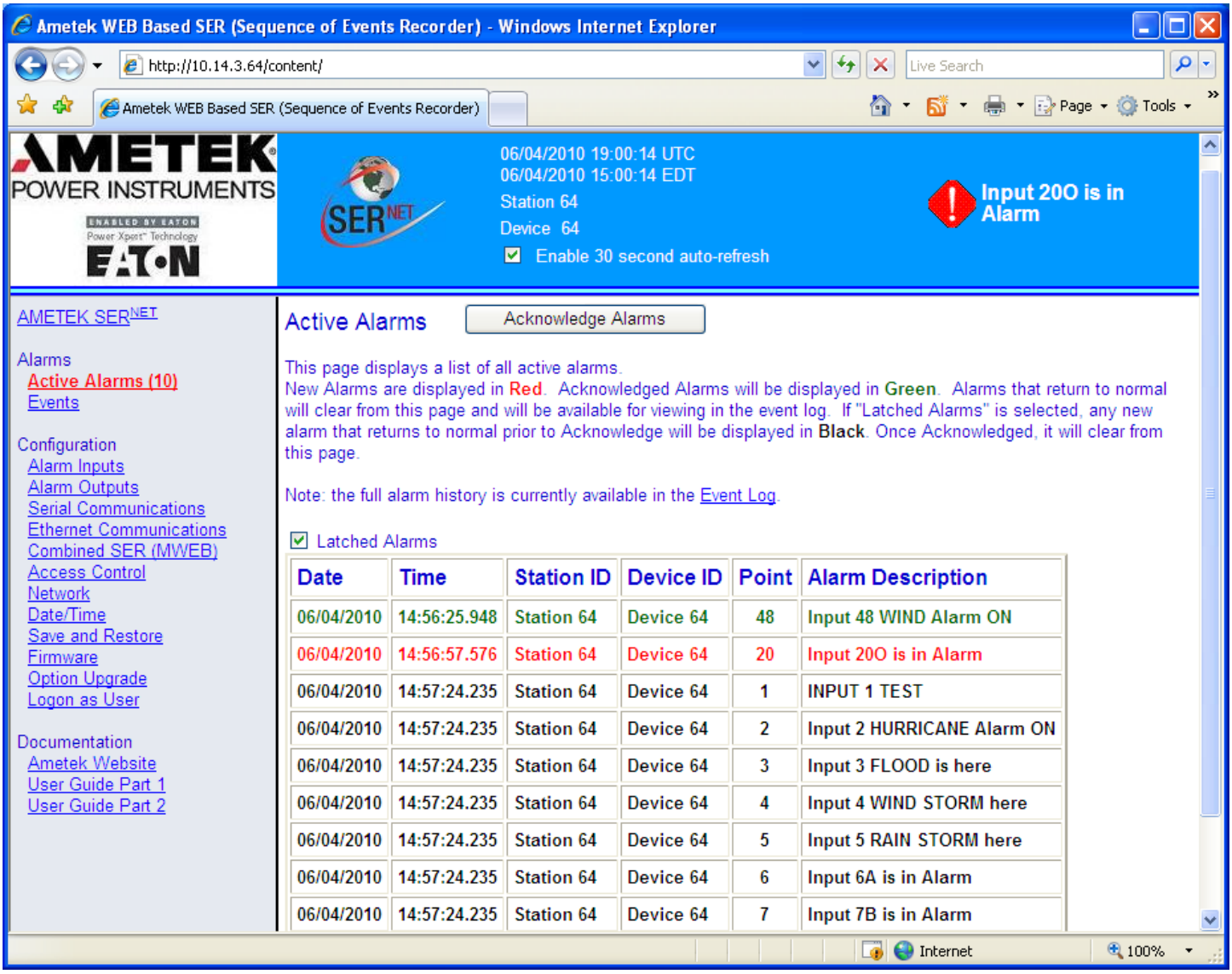


Figure 3–5. Active Alarms (#)

As shown in figure 3-5, the Active Alarm page displays all active alarms in chronological order as they occur. The active alarms can be latched by selecting the 'latched alarms' box or unlatched. The alarms can be color coded to show the various alarm states: Alarm, Acknowledged and Normal. Customizing the color schemes is done through the 'Color Selection' menu described later in the manual.

In Figure 3-5, Alarms are shown in Red, latched alarms that returned to normal before they were acknowledged are shown in Black and active alarms that have been acknowledged are shown in green. Different colors can be selected in the color selection configuration screen.

Unlatched Alarms

New alarms are shown in a user selectable color and displayed in chronological order. They will automatically clear from this screen and be saved in memory when they return to the normal state. Active alarms that have been acknowledged will change from red to green.

Latched Alarms

New alarms are shown in a user selectable color and displayed in chronological order. Active alarms that have been acknowledged will change colors. If an alarm returns to normal before it has been acknowledged, it will change to a different color. After an alarm has been acknowledged and the input has returned to normal, it will clear from this screen and be saved in memory.

Some SER^{NET} models have an LED indicator provided for every input. New alarms will flash the LED indicator. When the alarms are acknowledged, the LED will go from flashing to steady on. Alarms that return to normal will turn the LED off. The Acknowledge function will also de-activate the horn output if equipped.

Note: If the Acknowledge Function does not operate as indicated above, check your browser settings as shown in Appendix F.

Event Log Page

The Event log is used to view, sort, filter, print and download all alarms in memory. This will include IEC61850 points if the SER^{NET} has that feature enabled. Each SER^{NET} unit can store up to 40,000 events. When equipped with the MWEB option, the Master SER^{NET} will display events from itself as well as every slave SER^{NET} connected to it, in chronological order. An event can be an input going into alarm, returning to normal, diagnostic message and time synchronization status.

The event log is used to perform alarm management by filtering the list to a specific date and timeframe, sorting them by chronological order to determine the exact sequence of events for root cause analysis. In addition, events can be filtered to a specific input number or group of numbers to trend the number of occurrences within a given time frame. The event log can be downloaded for further analysis and data manipulation.

As shown in Figure 3–6, the Event Log displays all active and archived alarms, system status and diagnostics. In addition, the Event Log provides various sorting and filtering options and the ability to download or print events.

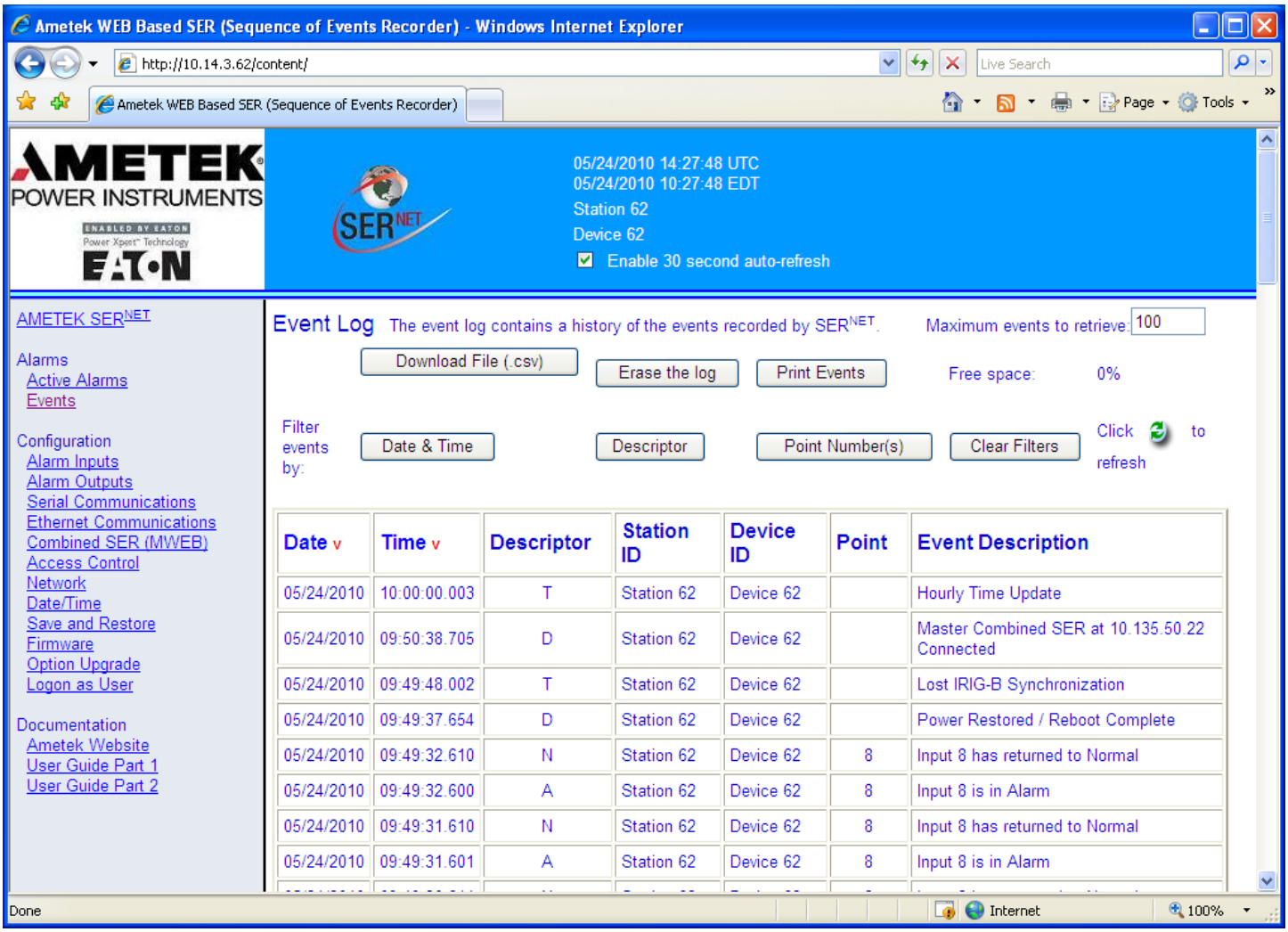


Figure 3–6. Event Log, Filtered by Events: Time (T), Diagnostic (D) & Input Return to Normal (N):

The different types of events are identified with a descriptor as shown in the table below.

Event Types	Event Descriptor	Event Description
Alarm Event	A N	Input goes into the Alarm State Input Returns to Normal State
Diagnostic Event	D	System Diagnostic for: -Unit Configuration -Disabled Alarms (Manual or Automatically) -Acknowledged Alarms -System Watchdog Faults *Refer to Appendix I for a complete list of diagnostic events*
Time Event	T	Event associated with Time Clock -Time Sync enabled -Time sync lost -Time Reset

Alarm Events will include a date, time (to millisecond), event descriptor (A or N), Station ID, Device ID, Point # and Event Description.

Diagnostic and Time Events are logged by date, time (to millisecond), event descriptor (D or T), Station ID, Device ID and Event Description.

The Time Event Descriptions (Event Descriptor T) will consist of:

- Time sync lost or locked
- Time resync for old or new time
- Restart date or time after SER is power cycled
- Hourly time update
- Time reconfigure

At the top of this page you will find action buttons for downloading to a .csv file, erasing and printing the log and setting the filters. The options are described below.

Download File (.csv)

If you want to save a copy of the events log to your pc, click this button. As shown in Figure 3–6, after you click the Download .csv button you may see a yellow warning bar across the top of the window. If so, follow the steps in Appendix F to configure your browser. If not, you will be prompted with a Script Prompt asking you if you want to download all events. Answering *Yes* will download all events, *No* will download only the events in view (with filters applied). Next you'll be prompted with the dialog box (Fig. 3–7) to open or save this file. Either open the file to view it, or select a folder where to save it. If you open the file, typically MS Excel® will open displaying the events in tabular form. From Excel® you can print the file in that form. Printing with the "Print Events" button will print the list as seen in the browser.

Note: There is a maximum of 1,000 events that you can view through the browser. To obtain a copy of all events (up to 40,000), you must answer *yes* after you click the *Download File* button.

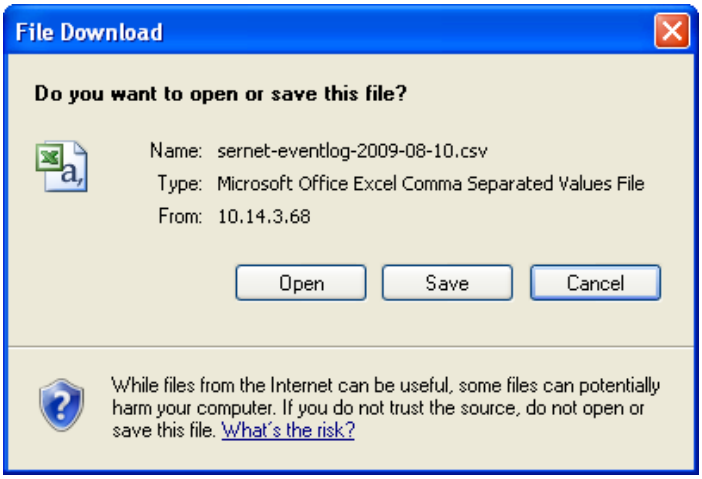


Figure 3–7. Save .csv File Dialog Box

Erase the log

Use caution, as this will permanently wipe out all events in the log. Under a User login, this option is grayed out. The event buffer stores a maximum of 40,000 events in non-volatile RAM. Events are automatically deleted on a FIFO basis (First In, First Out).

Print Events

Click here to create a printout of the events in the current view. It will print as viewed on the web page. If you first open the file in Excel® and then print, it will be more compact (more information per page) since the file will be in a tight tabular layout, typical of MS Excel®.

Maximum events to retrieve

The SER^{NET} Event Buffer can store 40,000 events. The number of events displayed at any one time can be selected by entering the number in this text box, (top right), followed by clicking the  icon to refresh the page with the desired number of events. A range of 1 – 1000 of the most recent events are allowed in this entry. Depending on how you sort and filter the list of events, it could be the most recent group of events or oldest alarms stored in memory.

Event Sorting and Filtering

Event Sorting

The column headings are active elements, meaning you can click on the column heading to change the sorted order of the events. It works similar to the column headings in Windows explorer. An arrow will appear, next to the heading title, toggling up and down each time you click the heading. For example, each time you click the Date column heading, the events are resorted chronologically or in reverse. Depending on the number of events, this could take a few seconds to change.

Filter Events by:

The Event Log can be filtered to only show alarms within a given date and time, specific event types and specific inputs.

You can combine 2 filters at one time to obtain an even more selective set. The following combinations of filters can be entered:

- Date & Time and Descriptor
- Date & Time and Point Number

When a filter is active, the filter criteria are displayed above the events table. See the following figure which is filtered by Date, Time and Point number.

Date & Time

To set date/time filters, click the Date & Time button on the page. This brings up the dialog box shown in the following figure. The events will be displayed according to your selection criteria. The default entry shows the current Date/Time range of the events currently in view.

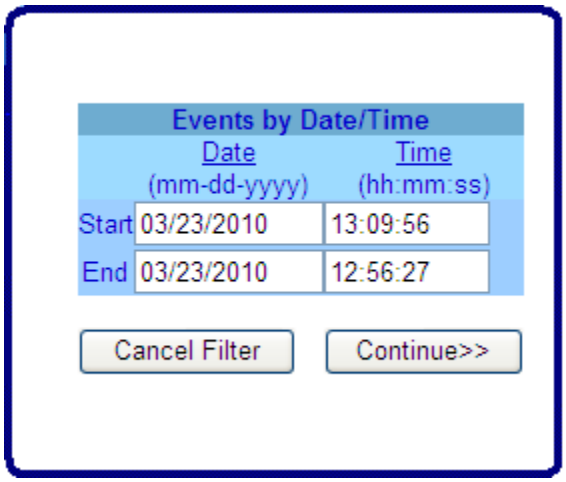


Figure 3–8. Date/Time Filter Dialog Box

Descriptor:

In this dialog box you can set what descriptors you want to display in the event log. Multiple descriptors may be selected. Place a check in the appropriate check box to enable that option. Please refer to the following figure.

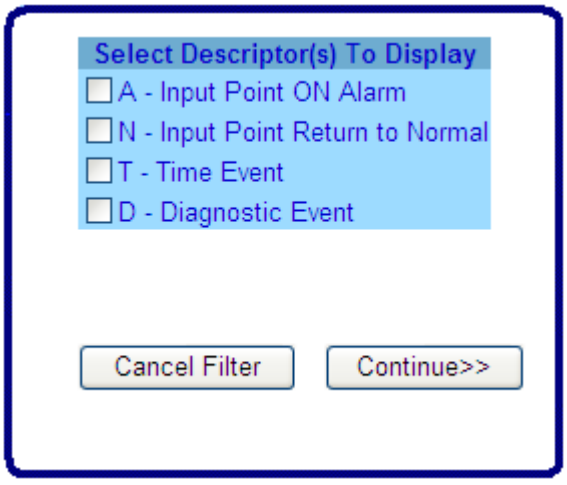


Figure 3–9. Descriptor Dialog Box

Point Number(s):

Here you can set which points you want displayed in the events list. Multiple points may be selected by using a comma between input numbers.

Figure 3–10. Points Dialog Box

The *Clear Filters* button will remove the event filters that you configured and displays the latest events.

Note: The Event Log Display does not automatically add new alarms to the list of events unless manually refreshed. If the Event Log does not update the list of alarms containing new events after you Refresh or when first selecting this display, check your browser settings as shown in Appendix F.

WEB Browser System Configuration

The SER^{NET} is configured through the web browser. The configuration consists of setting up the alarm inputs and outputs, setting the time and date and the device communications. All configuration items require a log-in of administrator. A user log-in will let you view the configuration, but not make any changes. Following is information on the different configuration pages. Please refer to the following figures.

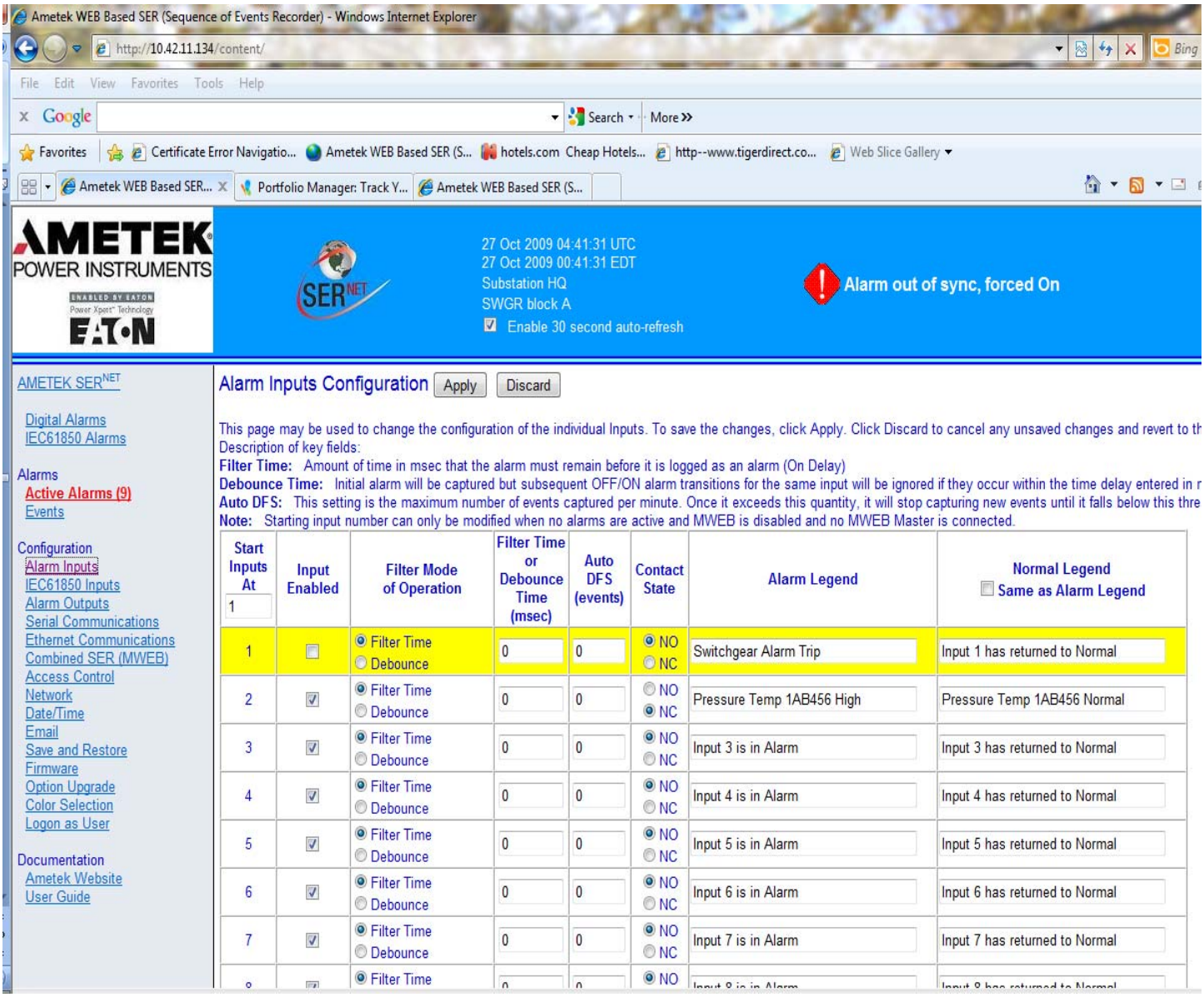


Figure 3–11. Alarm Inputs Configuration Page

Alarm Inputs Configuration

This configuration screen will display the quantity of input channels in your SER^{NET} model from 16 to 48 inputs..The configuration allows you to configure the contact alarm state for: NO (Normally Open, Customer contact closes on alarm) or NC (Normally Closed, Customer contact opens on alarm). In addition, you can configure a filter for each input and a unique legend that is used to describe the alarm or normal state.

Input

The input number is included with every alarm and return to normal event. The default input number will start at 1. It can be changed to start on any input and will automatically increment all subsequent input numbers.

When multiple SER^{NET} units are used in a system, it may be necessary to increment the input numbers, so you don't end up with the same input number on different systems. When the MWEB option is used (allows you to collect alarms from up to 24 SER^{NET} units and display them on a single SER^{NET} unit) the unit with the MWEB feature is designated as a Master and must start the input numbering at 1. The first slave unit would then start after these input numbers.

Example 1: 1-48 on Master SER^{NET}, 49-96 on Slave SER^{NET} Unit 1, 97-144 on Slave SER^{NET} Unit 2, etc.

Note: Before enabling the MWEB feature on the Master, the Slave unit input numbers must be assigned.

Nuisance Alarms

False alarms can fill up the event buffer and get in the way of critical alarms that need to be acted upon quickly. Several tools are provided to eliminate these false alarms and keep the list of archived events more manageable.

Input Enabled

You have the ability to disable alarms that may be out for service. Once disabled, they will no longer indicate an alarm regardless of the input state. Disabling and re-enabling alarms will be noted in the event log.

Filter Mode of Operation:

Input Filters are typically used to screen out momentary (false) alarms and Debounce Filters are used to eliminate repetitive alarms from a chattering contact. The Automatic Delete from Scan function is used to disable a repetitive alarm for a period of time until it settles down and then record it when it finally stays in the alarm state.

Filter or Debounce Time:

Values can be 0–65535ms. 0 defaults to 1ms input response if the filter mode is "Filter Time". This value is the time that the alarm must be present before an alarm is registered. For example, if you set the time to 200ms, then the contact must stay in alarm for 200ms before it is registered. Once it exceeds the filter time, the alarm will be recorded using the time stamp when it first went into the alarm state.

The SER^{NET} has a built-in filter to screen out sub-millisecond contact bounce or noise. Each Input requires 4 continuous successful samples (at 0.5 msec each) before an alarm is captured. Time stamp is recorded at first successful sample of the 4. Once an alarm is recorded, it can be configured to eliminate repeat contact bounce lasting 0-60 seconds. If the filter mode is set to "Debounce", active alarms will be prevented from multiple occurrences for the set time period. For example, if you set the Debounce time to 200 ms and the contact goes in alarm but toggles on and off 100 ms apart for several seconds before eventually staying in the alarm state, only one alarm will be recorded with a timestamp when it first went into the alarm state.

Auto DFS (Delete From Scan):

Values can be from 0–255 per minute. 0 = no delete from scan. For example if a contact toggles on and off X or more times per minute (depending on your setting) it is deleted from the scan. And that contact will not be registered. Once a contact toggles on/off below the set rate, it will be automatically re-inserted into scan.

Contact State:

Depending on the contacts used, set the contact for NO (Normally Open) or NC (Normally Closed).

Alarm Legend:

You may identify each input with a specific description. If no description is entered, the default will be Input # is in Alarm. The Alarm Legend will be displayed on the SER^{NET} Home Page Annunciator Graphic, Active Alarm Page, Event Log page, event download, ASCII output and printouts.

Normal Legend:

The Normal Legend will be displayed when the input has cleared. And it will be displayed on the SER^{NET} Home Page Annunciator Graphic, Active Alarm Page, Event Log page, event download, ASCII output and printouts. If you click the *Same as the Alarm Legend* check box, the description will mirror the Alarm Legend. And nothing will be displayed in this column.

External Acknowledge Pushbutton Input

The last input to the system can be configured as an Acknowledge Pushbutton input as shown in figure 3-12a. When configured for this, the pushbutton can perform the same functionality as the Acknowledge button on the WEB Browser, such as acknowledging alarms on various screens, changing the LED indicators on the SER^{NET} unit from flashing to steady and de-activating a horn output if used.

Set all Inputs

(at bottom) To set an entire column to the same setting, enter the value and press the tab key. You will be prompted to set all settings to the same value. This can save you time rather than setting each input individually.

Import / Export Legends

As shown in figure 3-12a, the legend import / export allows you to upload or download legends from a csv file. To see the csv file format, refer to Appendix J. Or, simply export the default legends configured into the SER^{NET} and you will see the required format in your csv file. Also, the instructions are included in the csv export file for reference.

Note: The legend format matches the ISM SER format for legends. When transferring the legends from an ISM system, export the legends from the ISM and then import that file into the SER^{NET}.

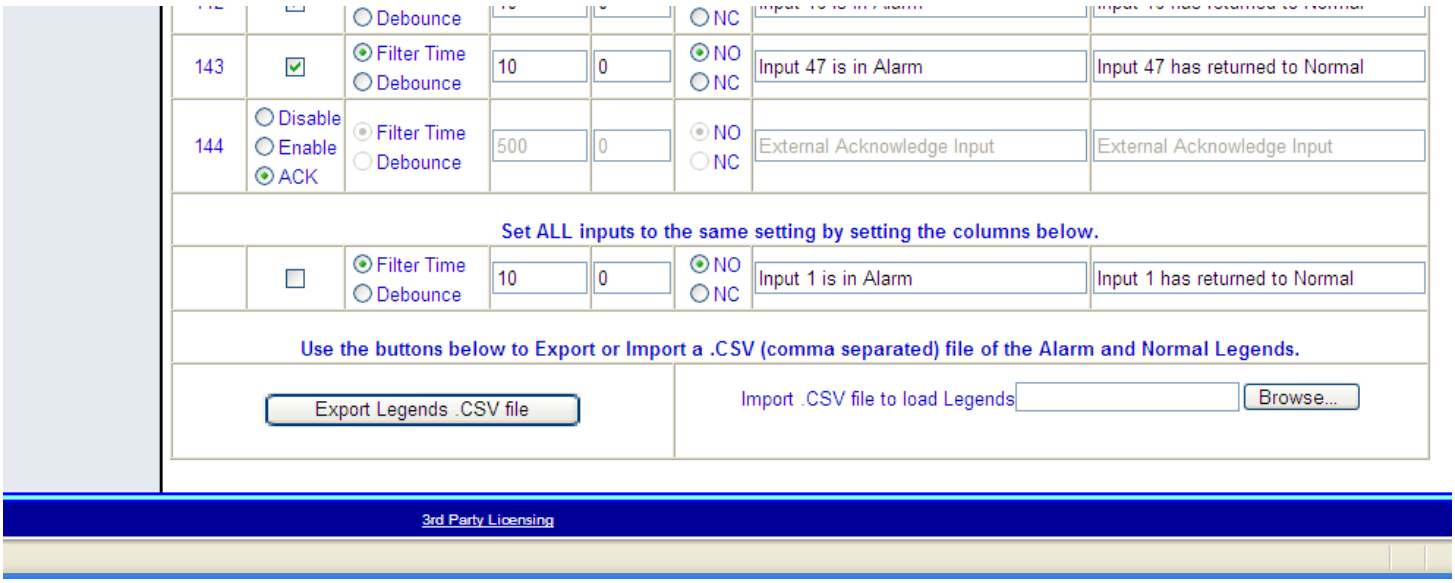


Figure 3-12a Import / Export Legends

Once you are finished with the settings, click *Apply* (must be logged in as Administrator)

IEC61850 Inputs Configuration

For systems that include the IEC 61850 option, the inputs can be configured on the SER^{NET} as follows. As shown in figure 3-12b, this configuration screen will display the quantity of IEC61850 points in your SER^{NET} model from 16 to 48 inputs..The configuration allows you to enable or disable each IEC61850 input. In addition, you can configure the time stamp source, a filter for each input and a unique legend that is used to describe the alarm or normal state.

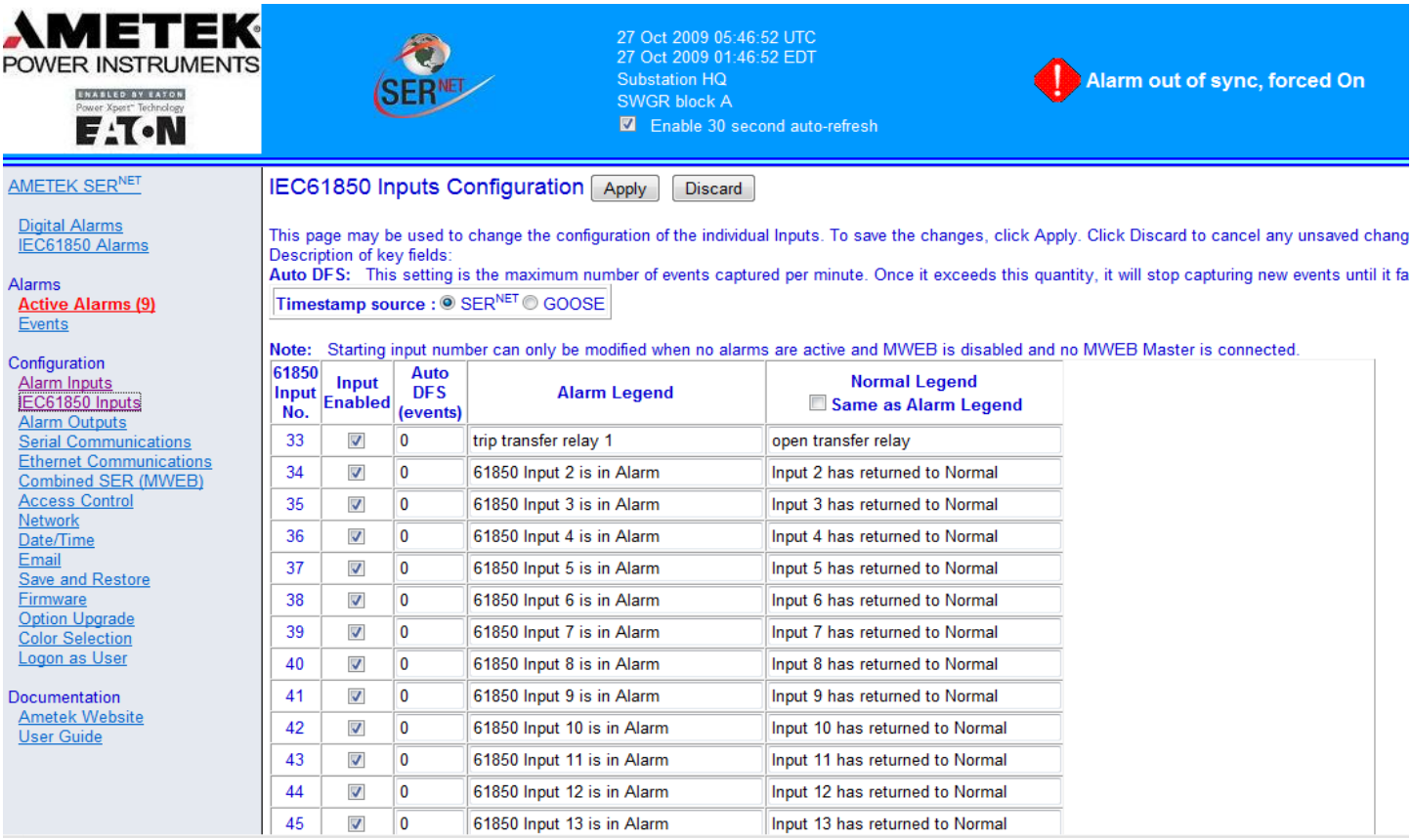


Figure 3-12b IEC 61850 Input Configuration

Input

The input number is included with every alarm and return to normal event. The default IEC61850 input number will start one point after the last Alarm Input point. See Figure 3-12c

SER^{NET} Model	Digital Input Numbering	IEC 61850 Input Numbering
16	1-16	17-32
32	1-32	33-64
48	1-48	49-96

Figure 3-12c IEC61850 Input Numbering

When multiple SER^{NET} units are used in a system, it may be necessary to increment the input numbers, so you don't end up with the same input number on different systems. When the MWEB option is used (allows you to collect alarms from up to 24 SER^{NET} units and display them on a single

SER^{NET} unit) the unit with the MWEB feature is designated as a Master and must start the input numbering at 1. The first slave unit would then start after these input numbers.

Example 1: 1-48 on Master SER^{NET}, 49-96 on Slave SER^{NET} Unit 1, 97-144 on Slave SER^{NET} Unit 2, etc.

Example 2: - IEC61850 Enabled: 1-48 (Alarm Inputs), 49-96 (IEC61850 Inputs) on Master SER^{NET}, 97-144 (Alarm Inputs), 145-192 (IEC61850 Inputs) on Slave SER^{NET} Unit 1, 193-241 (Alarm Inputs), 242-288 (IEC61850 Inputs) on Slave SER^{NET} Unit 2, etc.

Note: It is not necessary to have IEC61850 enabled on all units within the MWeb system. Before enabling the MWEB feature on the Master, the Slave unit input numbers must be assigned.

Timestamp Source:

The IEC61850 alarms can be time stamped by the SER^{NET} receiving the alarms or by the IED sending the alarms. The selection of the desired time stamp source is made by selecting the appropriate bullet in the IEC61850 Input Configuration page.

Input Enabled

You have the ability to disable alarms that may be out for service. Once disabled, they will no longer indicate an alarm regardless of the input state. Disabling and re-enabling alarms will be noted in the event log.

Auto DFS (Delete From Scan):

Values can be from 0–255 per minute. 0 = no delete from scan. For example if a contact toggles on and off X or more times per minute (depending on your setting) it is deleted from the scan. And that contact will not be registered. Once a contact toggles on/off below the set rate, it will be automatically re-inserted into scan.

Alarm Legend:

You may identify each input with a specific description. If no description is entered, the default will be Input # is in Alarm. The Alarm Legend will be displayed on the SER^{NET} Home Page Annunciator Graphic, Active Alarm Page, Event Log page, event download, ASCII output and printouts.

Normal Legend:

The Normal Legend will be displayed when the input has cleared. And it will be displayed on the SER^{NET} Home Page Annunciator Graphic, Active Alarm Page, Event Log page, event download, ASCII output and printouts. If you click the *Same as the Alarm Legend* check box, the description will mirror the Alarm Legend. And nothing will be displayed in this column.

Set all Inputs

(at bottom) To set an entire column to the same setting, enter the value and press the tab key. You will be prompted to set all settings to the same value. This can save you time rather than setting each input individually.

Import / Export Legends

As shown in figure 3-12d, the legend import / export allows you to upload or download legends from a csv file. To see the csv file format, refer to Appendix J. Or, simply export the default legends configured into the SER^{NET} and you will see the required format in your csv file. Also, the instructions are included in the csv export file for reference.

Note: The legend format matches the ISM SER format for legends. When transferring the legends from an ISM system, export the legends from the ISM and then import that file into the SER^{NET}.

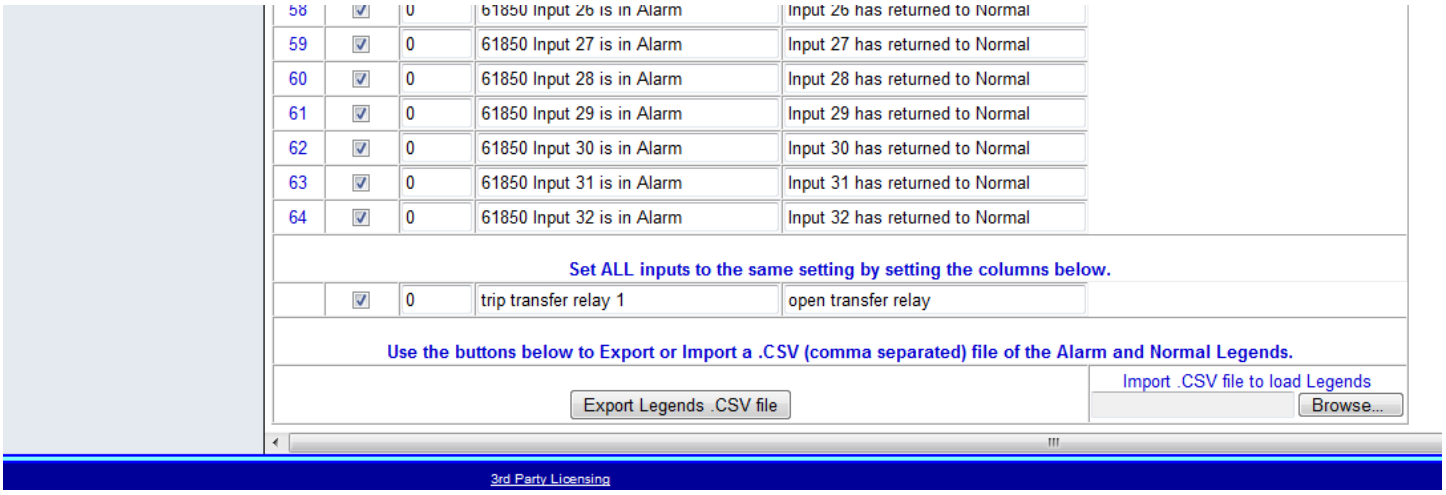


Figure 3-12d Import / Export Legends

Once you are finished with the settings, click *Apply* (must be logged in as Administrator)

Alarm Outputs Configuration

SER^{NET} has two Form C Relay outputs, Alarm Output 1 & 2. (Please refer to Figure 3–13).

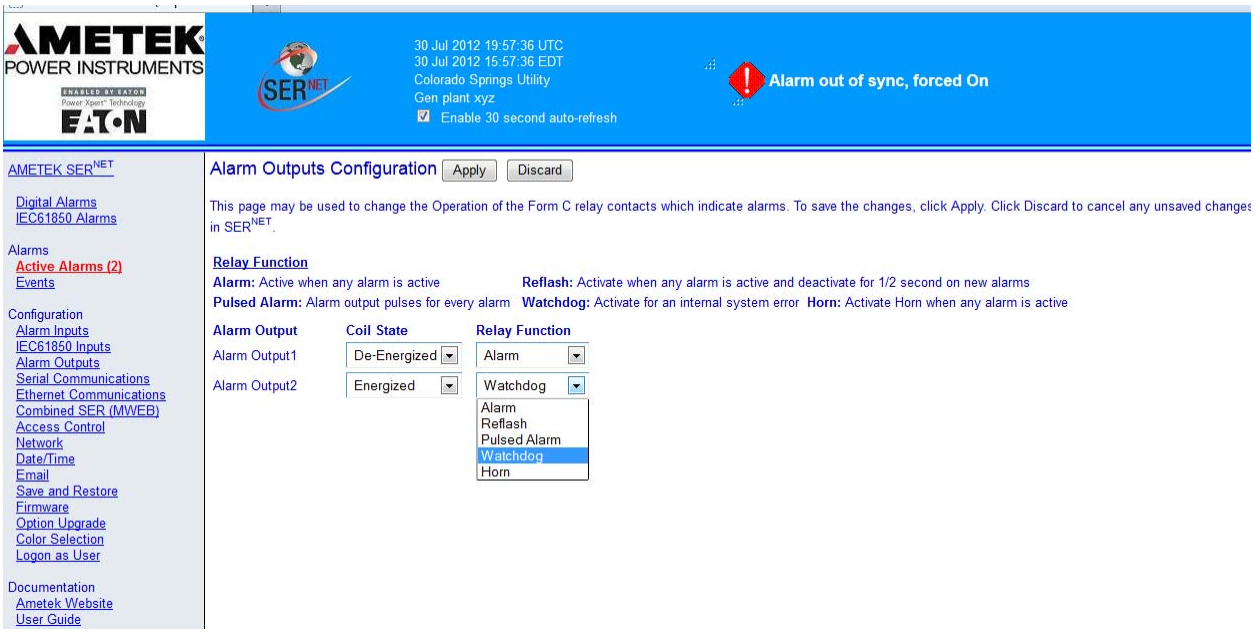


Figure 3–13. Alarm Outputs Configuration Page

Coil State

The Alarm Output Relay Coil can be configured to be energized or de-energized in the normal state.

Energized – The Relay coil is energized with power when normal and de-energizes when it is activated. This is most often used in fail-safe applications, where a loss of power will de-energize the relay coil and transfer the contacts.

De-energized – The Relay coil is de-energized when normal and energizes when it is activated.

Relay Function

The Relay Function can be set to any of the following:

Alarm –	Activate when any alarm is active
Reflash –	Activate when any alarm is active and pulse for ½ second for new alarms
Pulsed Alarm	Alarm output pulses for every alarm.
Watchdog –	Activate for an internal system error.
Horn	Activate when any alarm is active. Resets upon Acknowledge function.

After selecting your options click *Apply*.

Serial Communications Configuration

On this page, you configure the unit's Serial Communications parameters. These settings are dependent on the device to which you will connect. The serial port supports a single connection of either the optional Modbus RTU, optional DNP and standard Serial ASCII protocol. After you make your selections, click *Apply*.

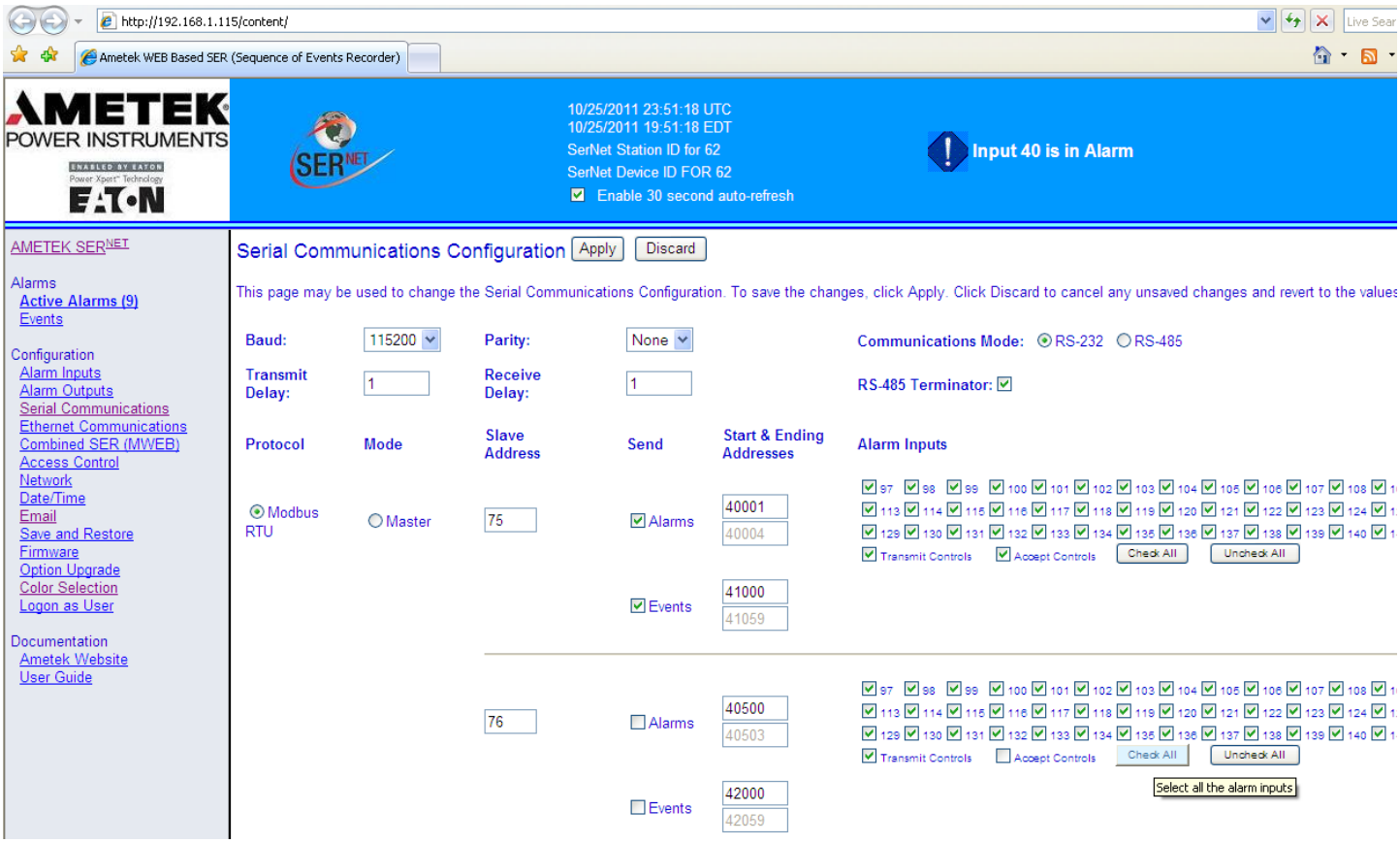


Figure 3–14a. Serial Communications Configuration Page (Top Half)

Communication Set-up:

Select the Baud Rate, Parity and communication delays to match your application.
The SER^{NET} has a single DB9 serial port that can be configured for RS-232 or RS-485 communication mode. Refer to Chapter 2 for RS-232 and RS-485 connections.

When using RS-485 to connect multiple devices together, the last unit must be terminated with the RS-485 Terminator checkbox.

Once your communications parameters are set, you can choose the type of output desired. They are as follows:

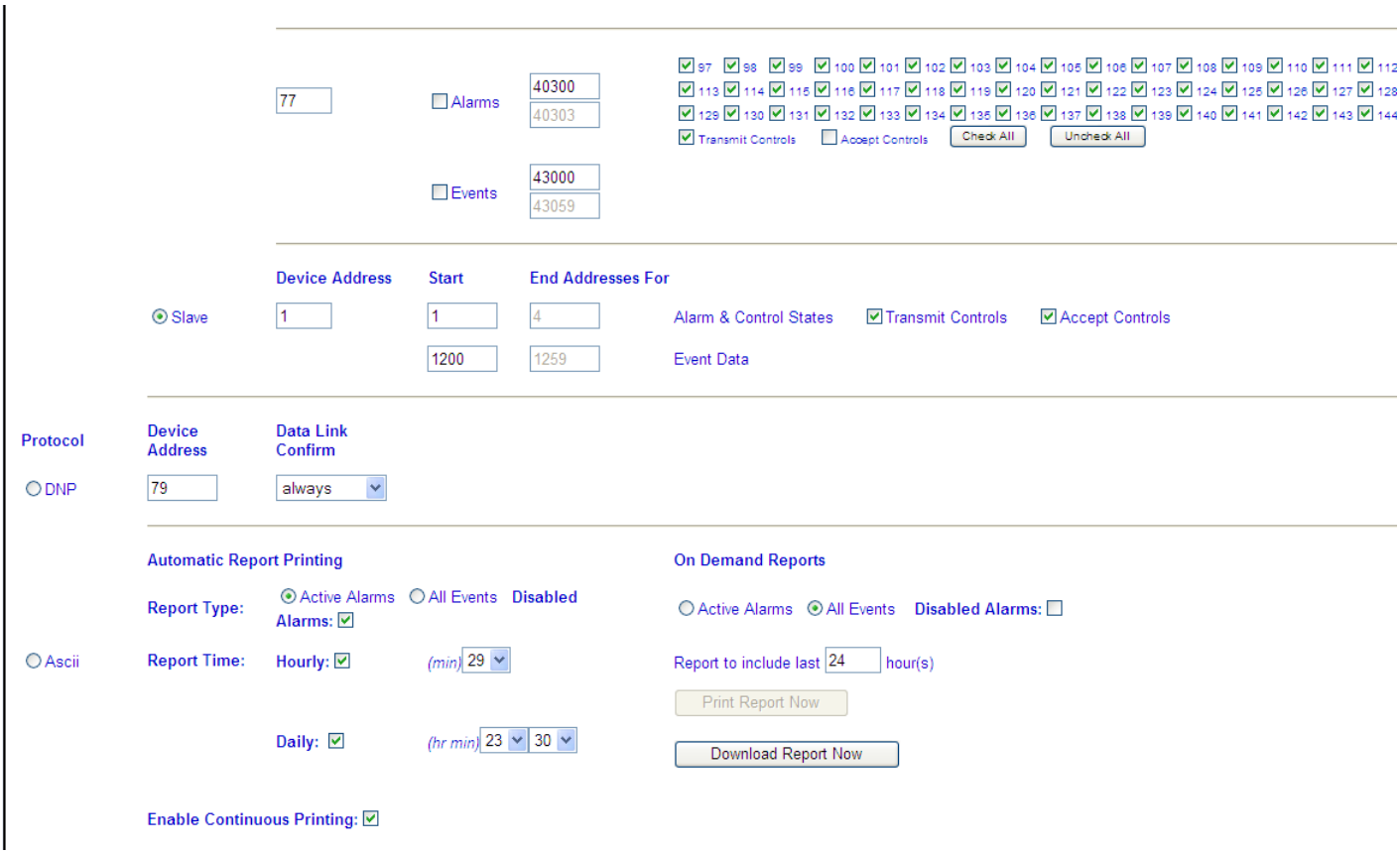


Figure 3–14b. Serial Communications Configuration Page (Bottom Half)

Modbus

The SER^{NET} Modbus port will transmit the status and timestamp of each alarm. The transmitted alarms can be used to drive an AMETEK Annunciator, RTU, SCADA, PLC or other device. Refer to Appendix A for detailed Modbus operation and mapping. The Modbus port supports device addresses of 1-255, a maximum Baud Rate of 115,200 and odd, even or no parity.

Modbus Master: The Modbus Port can be configured as a Master, with connection to up to 3 Modbus Slave devices. In this mode, you enter the Slave Address for each device you wish to connect to.

Select ‘Alarms’ to provide Alarm Status (On/Off status per input). Alarm Status is provided by reading 16-bit holding registers with a single bit designated per input. You can select all or specific inputs by checking the input number box. You can also provide the capability to accept a remote Acknowledge input or transmit the state of the unit’s alarm acknowledge function by selecting ‘Accept Controls’ or ‘Transmit Controls’. The Modbus Start address can be configured based on the application. The ending address will automatically be presented based on the number of inputs selected. Example: If all 48 alarms are selected, it will require three 16 bit registers, 32 alarms will require 2 registers, 20 alarms will require 2 registers, etc. The pushbutton controls will add an extra register to the list.

Modbus Alarm Mapping

Starting Register address: 40001, inputs 1-32 selected, inputs 1,15,18 on alarm

Register	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
40001	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
40002	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Starting Register address: 40001, inputs 1, 5, 9, 12, 21-48 selected, inputs 5, 12, 48 on alarm

Register	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
40001	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
40002	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Register 40001 & 40002 is a 16 bit holding register. The status of the 16 bits shown.
(Binary 0 = Normal, Binary 1 = Alarm)

Select ‘Events’ to provide alarm status with a time and date stamp. The Modbus interface requires six 16-bit registers for each event. 10 events are returned per poll for a total of 60 registers. The Modbus Start address can be configured based on the application. The ending address will automatically be calculated for the 60 registers required. Refer to Appendix A for complete details.

Systems with MWEB Option

With MWEB enabled, Modbus alarms will be sent for all inputs of the master, followed by all inputs of each remote SER^{NET}. Modbus will not operate before MWEB has made all possible connections to remote SER^{NET} units. During this time, you'll see a warning, as shown in Figure 3–14c.

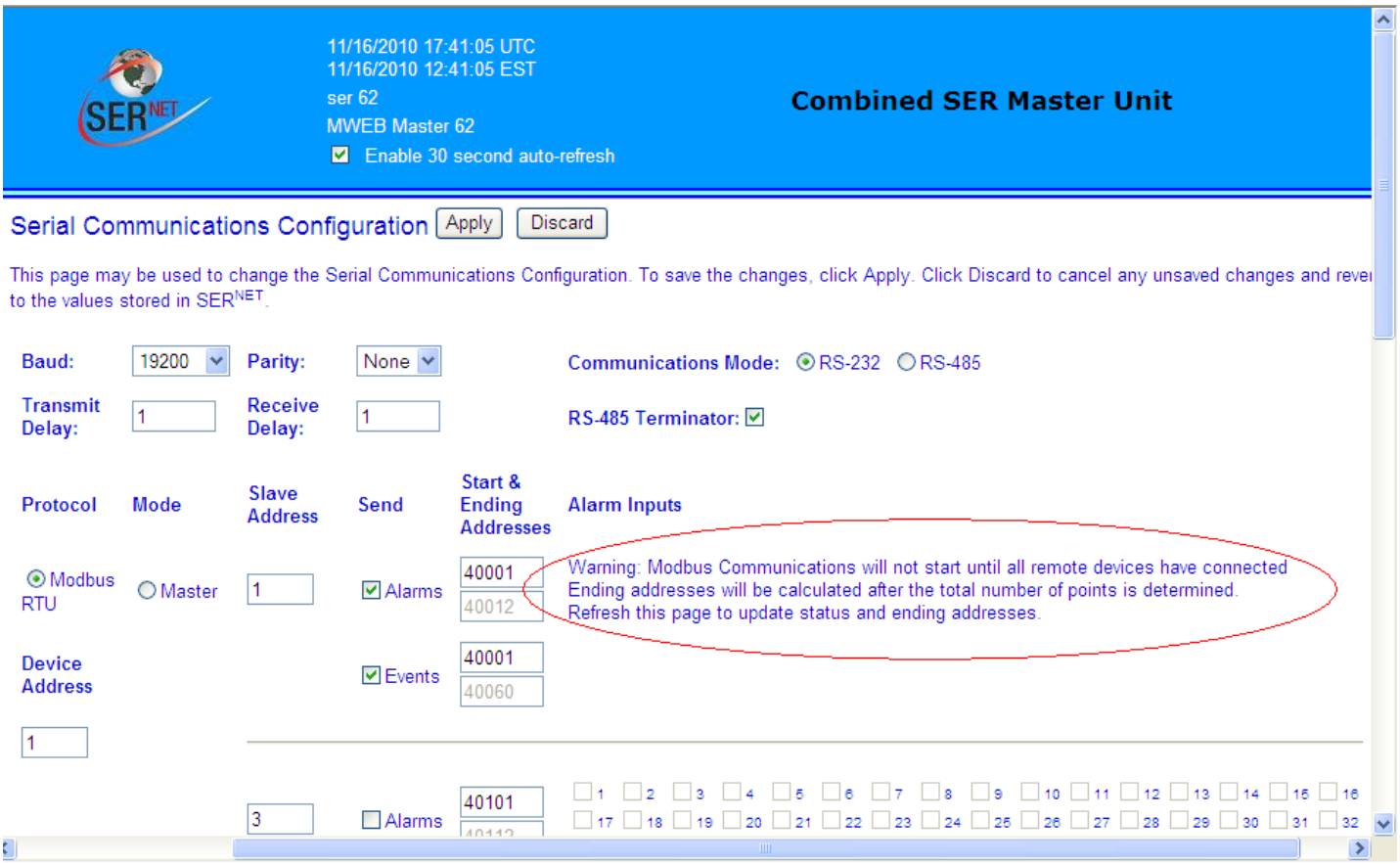


Figure 3–14c. Serial Communications Page Immediately after Enabling MWEB.

Warning: Modbus Communications will not start until all remote devices have connected.
Ending addresses will be calculated after the total number of points is determined.
Refresh this page to update status and ending addresses.

With the Modbus & DNP protocols, all point numbers throughout the network are contiguous and unique. Note that all remote devices must respond before the point numbers are assigned at each SER^{NET} slave unit. For example, with a 48-point master and two 48-point slave devices; points will be numbered 1–48 (Master), 49–96 (slave 1) and 97–144 (slave 2).. For the example case with 3 SER^{NET} units, the page will look like Figure 3–14d with the following message.

Modbus for MWEB is enabled and ready.
A total of 144 Points in 9 registers will be sent for alarm data.

Note: When you disable MWEB, the number of registers will change and you may receive Modbus exceptions.

You can also view the MWEB point numbering scheme any time from the Combined SER (MWEB) configuration page. The MWEB page shows all point assignments for the entire network.

Modbus Slave: When configured as a Modbus Slave, the SER^{NET} will return both Alarm Status and Events to the Start/Ending addresses that you can select. The alarm status addresses start at 40000, so an entry of 1 will be 40001. The events will start at a default of 40100. You can also provide the capability to accept a remote Acknowledge input or transmit the state of the unit's alarm acknowledge function by selecting 'Accept Controls' or 'Transmit Controls'

The Modbus register map is detailed in Appendix A.

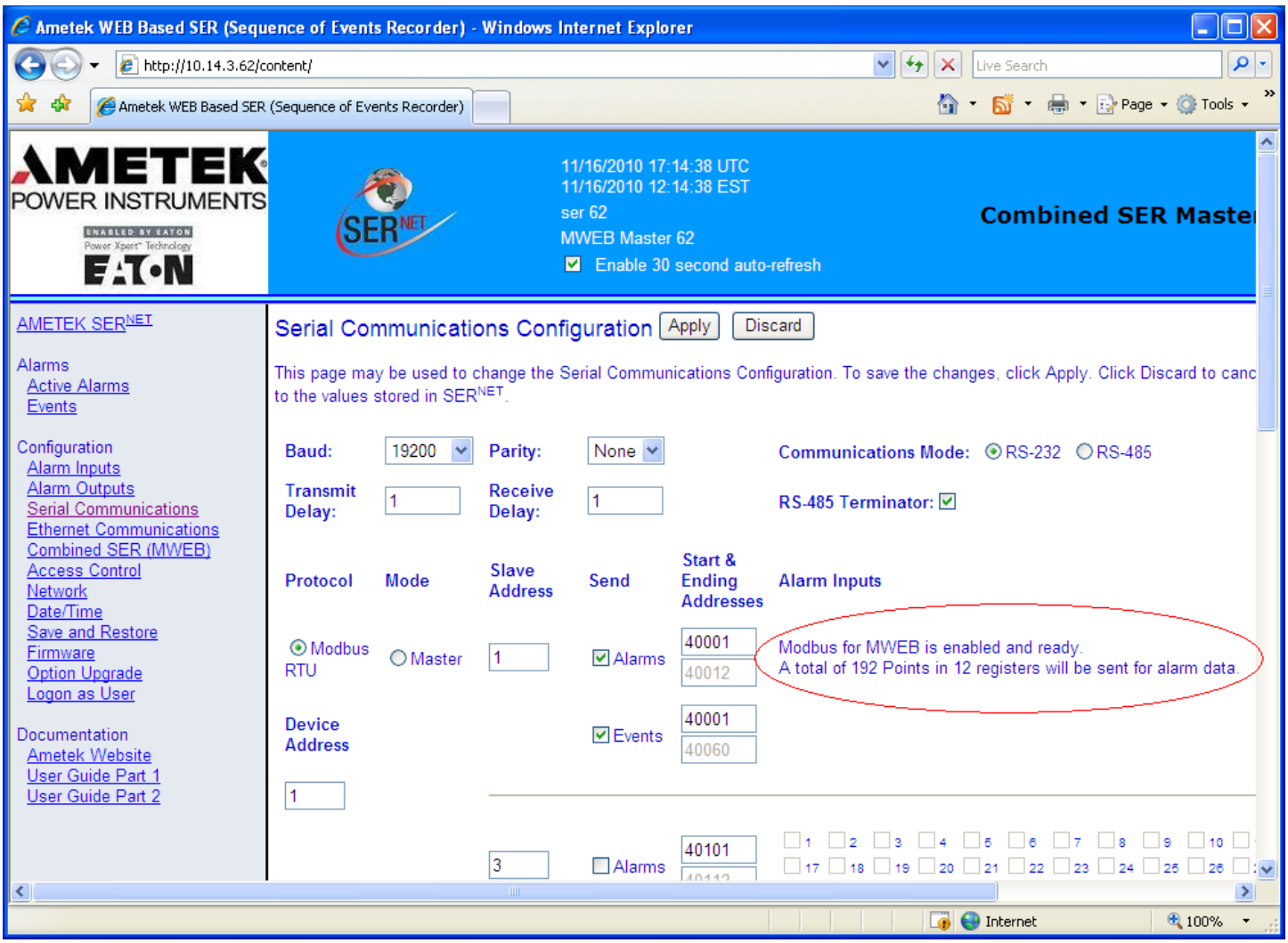


Figure 3–14d. Serial Communications Page with MWEB Enabled and Ready.

Systems with IEC 61850 Option

With IEC 61850 enabled, the Modbus output can transmit both the digital field contact input status as well as the GOOSE inputs received via IEC 61850. This allows you to re-transmit the IEC 61850 alarms into the Modbus Protocol.

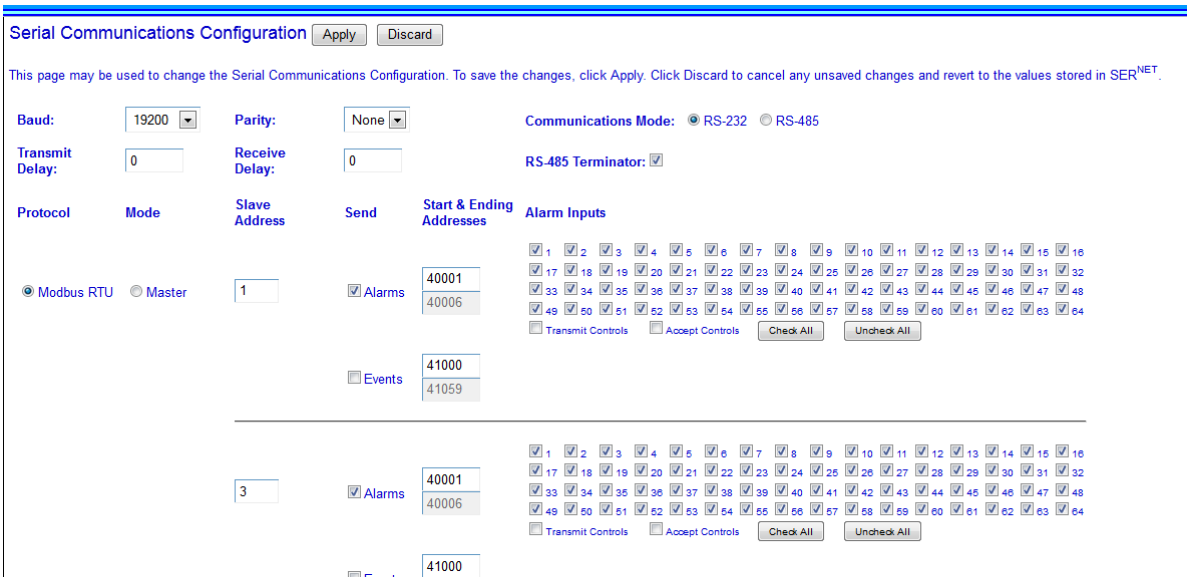


Figure 3–14e. Serial Communications Page after Enabling 61850

Modbus Alarm Mapping

When IEC 61850 is enabled, additional Modbus Registers are provided to transmit the IEC 61850 Input status. In the table below, a 32 input SER^{NET} with IEC 61850 will designate the first two registers for the digital inputs and the last two registers for the IEC 61850 Inputs.

Register	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
40001	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
40002	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
40003	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
40004	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

Registers 40001-40004 are 16 bit holding registers. The status of the 16 bits shown.
(Binary 0 = Normal, Binary 1 = Alarm)

As shown above, digital inputs 1,15,18 are on alarm as well as IEC 61850 inputs 2, 16 and 19.

The Modbus register map is detailed in Appendix A.

DNP

The SER^{NET} DNP port will transmit the status and timestamp of each alarm. The transmitted alarms can be used to drive an RTU, SCADA, PLC or other device.

If the IEC 61850 option is enabled, the GOOSE Inputs received via IEC 61850 can be retransmitted via DNP.

Refer to Appendix B for detailed DNP operation and mapping.

ASCII (Report Printing Times Serial Printer)

With the ASCII option, you can output the event log as they are entered. It is used for direct connection to a serial printer or terminal application. The output will resemble the Web browser display by order, columns etc. Sample reports are provided in the following figures. By selecting the appropriate radio buttons, and then entering your desired time criteria, you can sort the Alarms in a variety of ways:

Hourly – report alarms currently active or within the last hour.
Daily – report alarms currently active or for the entire day.
Active Alarms – report only active alarms.
All Alarms – report all alarms for the entire day.

If you enable continuous output, the SER^{NET} will output the events as they occur into the event log. If the master has the MWEB option (firmware V1.01+), all slave alarms will be included in the report.

None – disables communications protocol (Bottom of Fig. 3–14b).

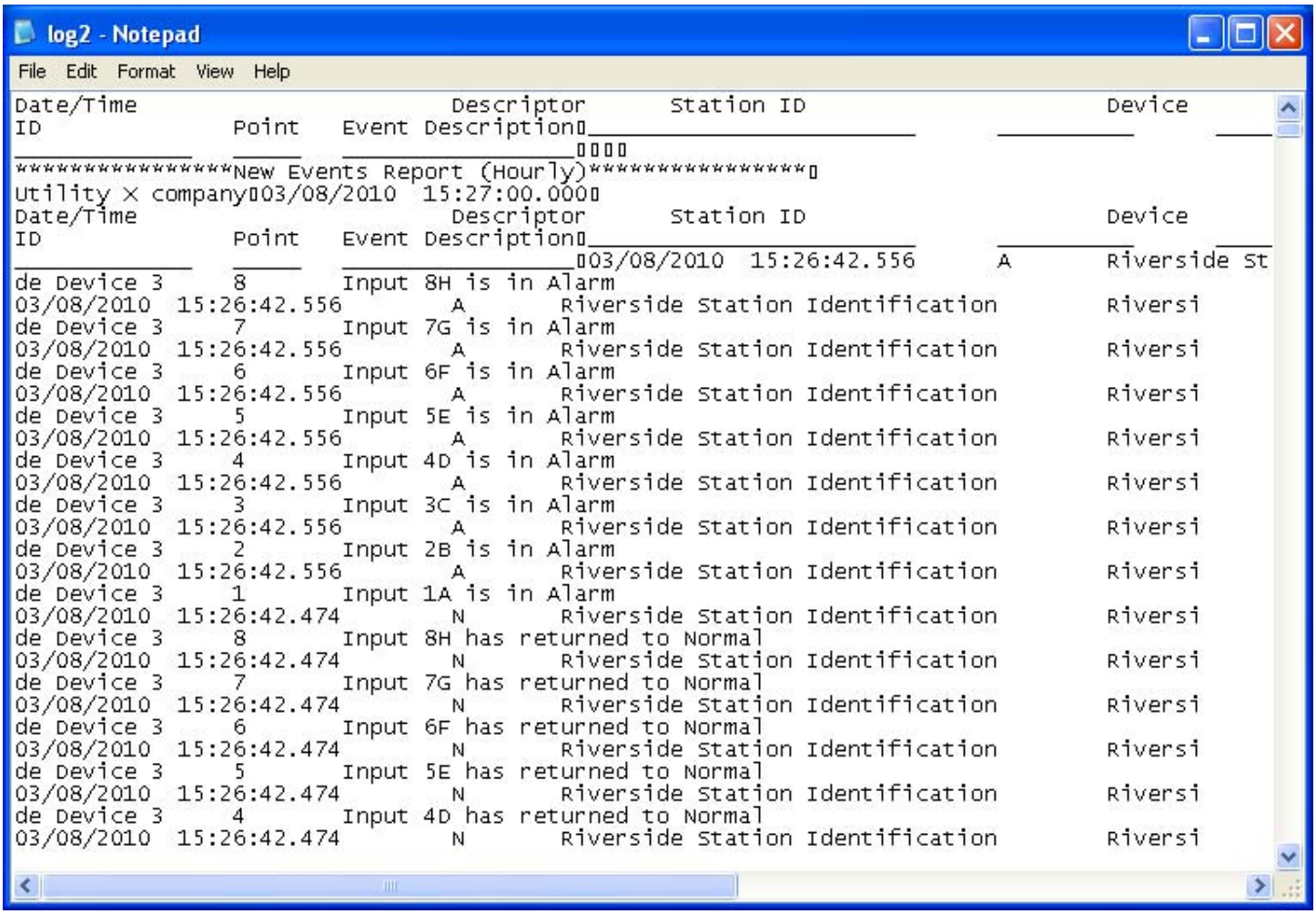


Figure 3–15a - Event Log Output in ASCII Format (Hourly).

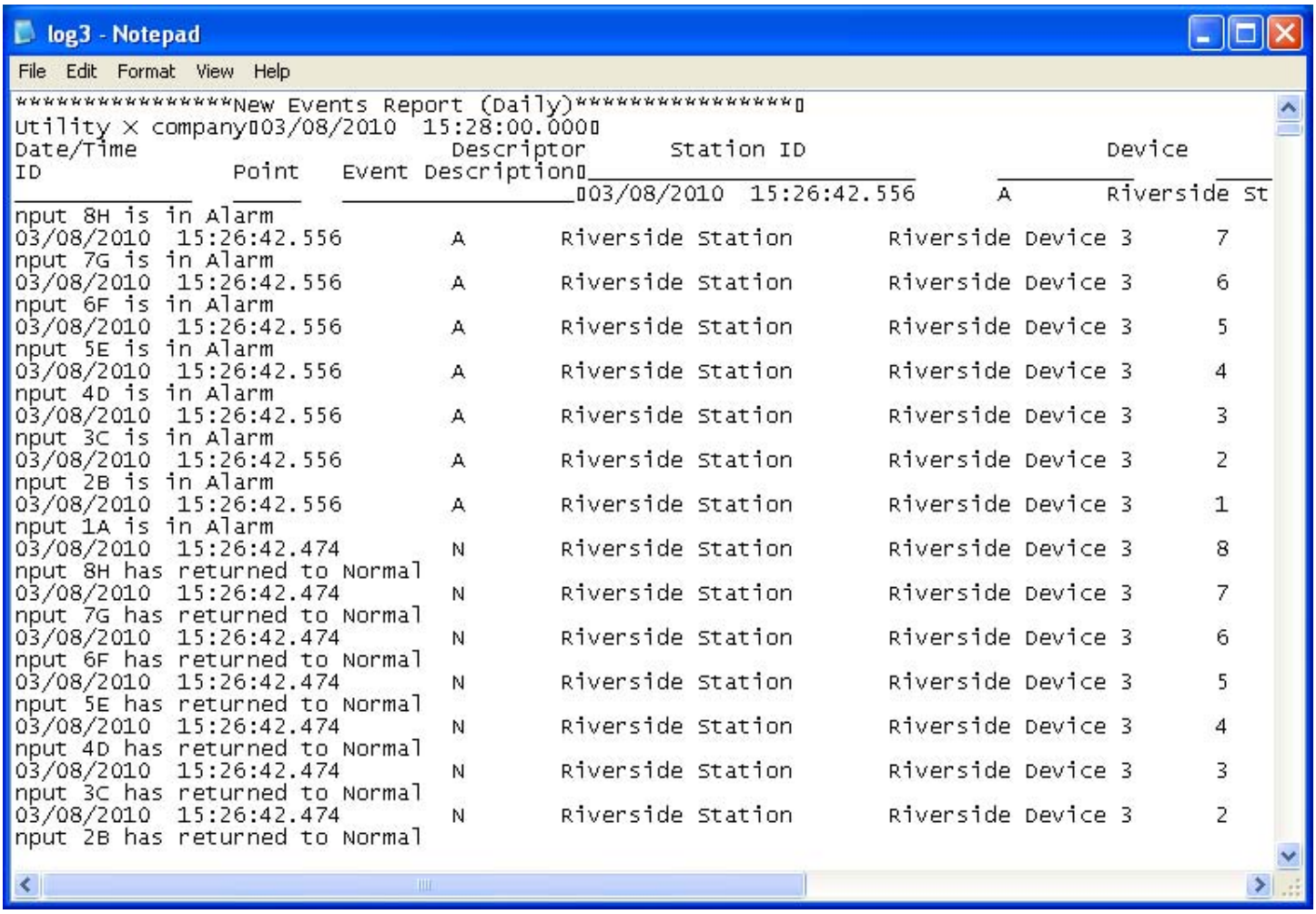


Figure 3–15b - Event Log Output in ASCII Format (Daily).

Ethernet Communications Configuration

On this page, you configure the unit's Ethernet Communications parameters. The Ethernet port supports 10Mbs or 100Mbs using simultaneous Modbus TCP/IP and DNP communication protocols.

The Modbus TCP/IP set-up is similar to the serial Modbus, except; you enter the Modbus TCP Port and when in Master Mode, you enter the IP addresses of the slave ports.

After making your changes, click *Apply*.

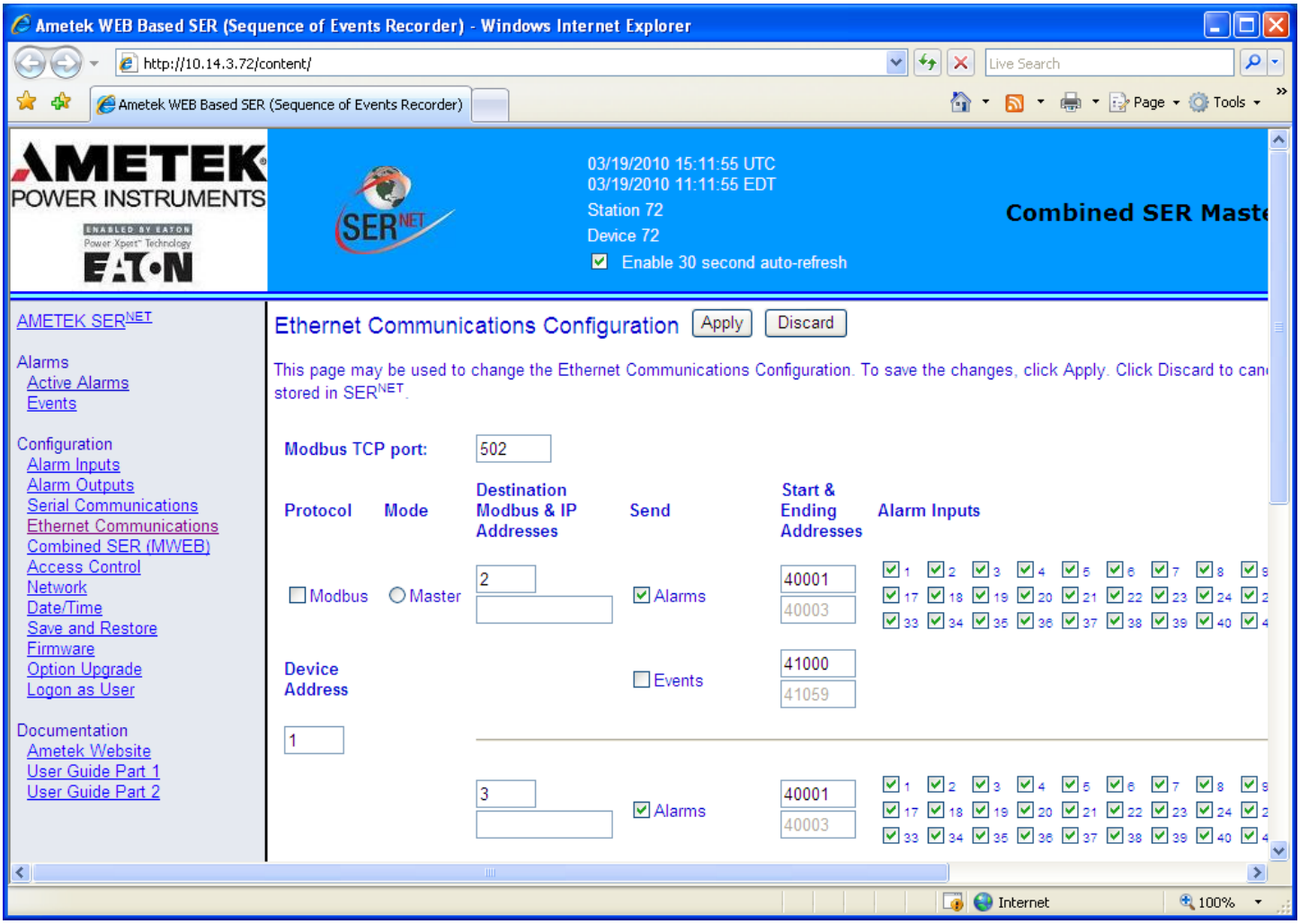


Figure 3–16a Ethernet Communications Configuration Page (Top Half)

Modbus

Set the Modbus TCP Port.
Choose which protocol you want to use.
Set the Mode (Master / Slave).
Configure the Destination IP Address.
Send Alarms and/or Events
Configure the Start and End Addresses.

Choose which Alarm Inputs you want to send (points).
Repeat for each slave.

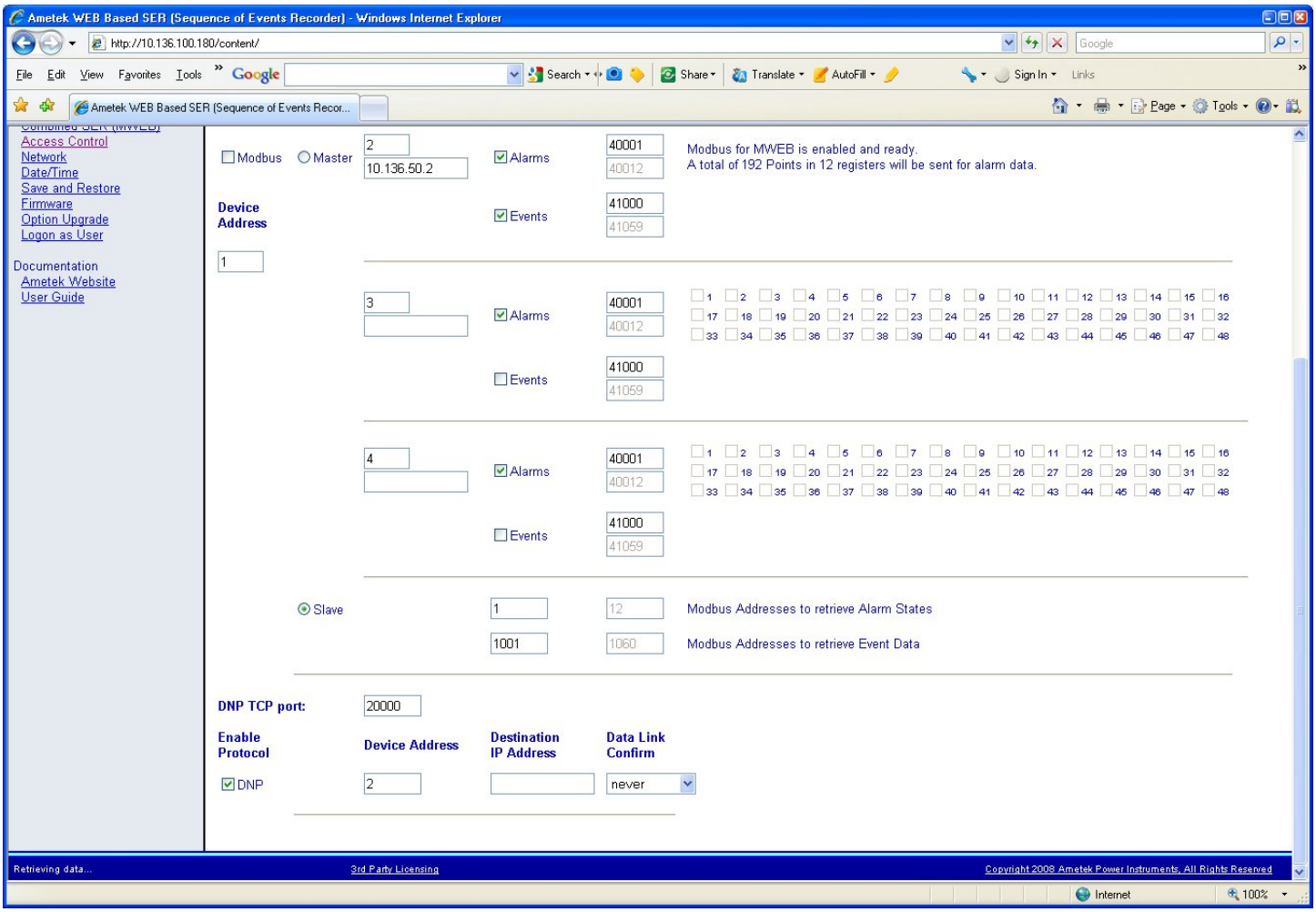


Figure 3–16b Ethernet Communications Configuration Page (Bottom Half)

With MWEB enabled, Modbus alarms will be sent for all inputs of the master, followed by all inputs of each remote SER^{NET}. Modbus will not operate before MWEB has made all possible connections to remote SER^{NET} units. During this time, you'll see a warning, as shown in Figure 3–14d.

Warning: Modbus Communications will not start until all remote devices have connected.
Ending addresses will be calculated after the total number of points is determined.
Refresh this page to update status and ending addresses.

With the Modbus & DNP protocols, all point numbers throughout the network are contiguous and unique. Note that all remote devices must respond before the virtual point numbers are assigned. For example, with a 48-point master and 2 48-point remote devices; points will be numbered 1–48 (Master), 49–96 (remote 1) and 97–144 (remote 2). This virtual point numbering scheme is automatically set up at the time MWEB is enabled and remains intact until MWEB is disabled. For the example case with 3 SER^{NET} units, the page will look like Figure 3–14d with the following message.

Modbus for MWEB is enabled and ready.
A total of 144 Points in 9 registers will be sent for alarm data.

You can also view the MWEB point numbering scheme any time from the Combined SER (MWEB) configuration page. The MWEB page shows all point assignments for the entire network.

DNP

The SER^{NET} DNP port will transmit the status and timestamp of each alarm. The transmitted alarms can be used to drive an RTU, SCADA, PLC or other device. .

Refer to Appendix B for detailed DNP operation and mapping.

Systems with IEC 61850 Option

With IEC 61850 enabled, the Modbus output can transmit both the digital field contact input status as well as the GOOSE inputs received via IEC 61850. This allows you to re-transmit the IEC 61850 alarms into the Modbus Protocol.

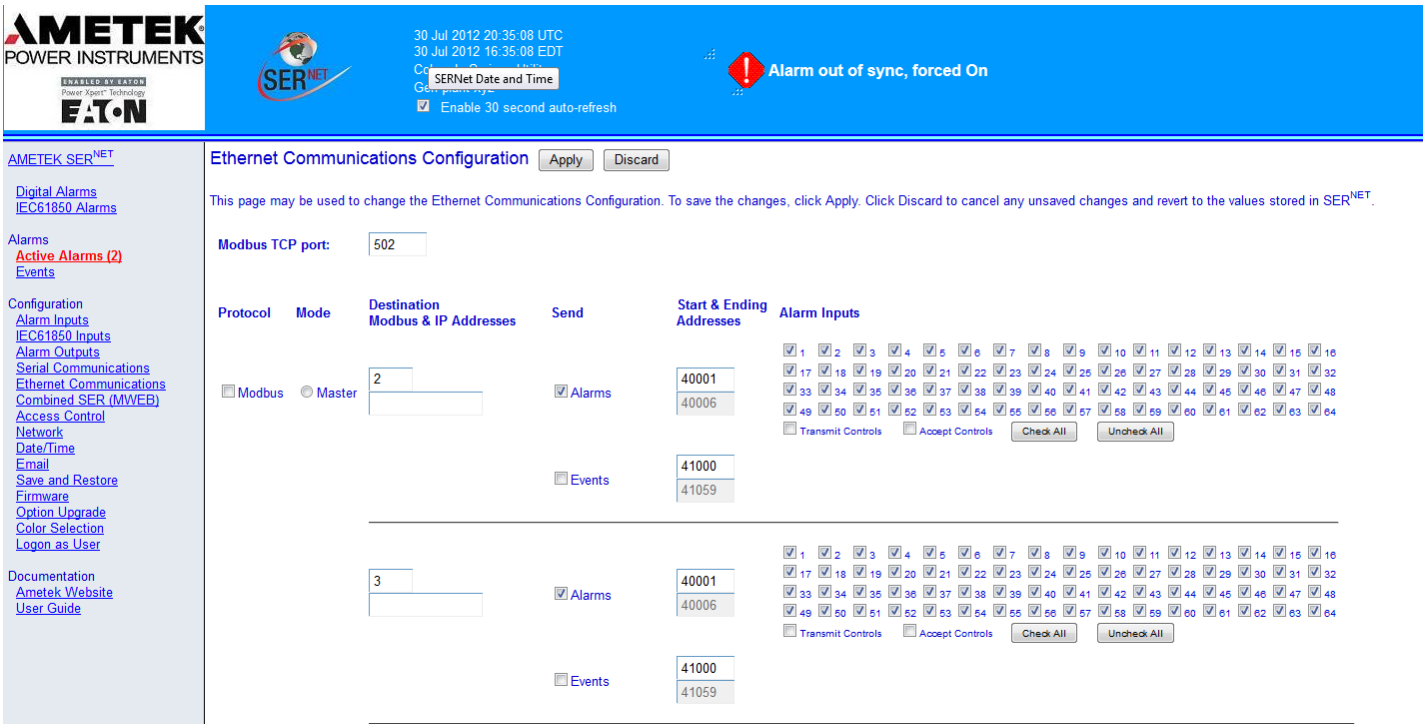


Figure 3–16c. Ethernet Communications Page after Enabling 61850

Modbus Alarm Mapping

When IEC 61850 is enabled, additional Modbus Registers are provided to transmit the IEC 61850 Input status. In the table below, a 32 input SER^{NET} with IEC 61850 will designate the first two registers for the digital inputs and the last two registers for the IEC 61850 Inputs.

Register	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
40001	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
40002	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
40003	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
40004	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

Registers 40001-40004 are 16 bit holding registers. The status of the 16 bits shown.
(Binary 0 = Normal, Binary 1 = Alarm)

As shown above, digital inputs 1,15,18 are on alarm as well as IEC 61850 inputs 2, 16 and 19.

The Modbus register map is detailed in Appendix A.

DNP

The SER^{NET} DNP port will transmit the status and timestamp of each alarm. The transmitted alarms can be used to drive an RTU, SCADA, PLC or other device.

If the IEC 61850 option is enabled, the GOOSE Inputs received via IEC 61850 can be retransmitted via DNP.

Refer to Appendix B for detailed DNP operation and mapping.

Combined SER (MWEB)

The Combined SER MWEB option (firmware 1.01+) enables a single SER^{NET} master to manage and collect alarms from up to 24 slaves. This master SER^{NET} can be used to view all alarms from the slaves in addition to alarms connected to the master using a single browser window. The master SER^{NET} can also transmit all alarms through the Modbus, DNP and ASCII communication protocols.

Before a SER^{NET} master is enabled with the MWEB option, you must first configure each SER^{NET} slave device with unique input numbers. The master SER^{NET} will start with input number 1 and the slave units will be numbered in succession. For example, if the master unit has 48 channels, the inputs will be numbered 1-48 and the first slave unit with 48 channels would be numbered 49-96, etc.

Note: If the slave unit inputs are not numbered in succession or if the input numbers overlap, the master SER^{NET} will not allow you to enable the MWEB option.

Once enabled, the master's pages will have "*Combined SER Master Unit*" in the top bar of each page, as shown in the following figure. The default state of a Combined SER MWEB unit is (Disabled) slave. The SER^{NET} unit must be enabled as a master by checking the enable checkbox on this page, then clicking the apply button. At the time the master is enabled, slave units will immediately send the current input states and all further changes to the master. In addition, the slave sends its active alarm states to the master every 2 minutes. If the master does not receive this periodic update from the slave, it will query the slave unit to determine if it has gone off-line. When a slave stops responding, the MWEB master removes all active alarms for this slave and re-attempts a new connection. Slaves may report to no more than 3 masters. For example, in a network of 20 units, one SER^{NET} unit can be master for all 20 units. One of the 20 units can be a master for 10 of the slaves. And a third master can show alarms from the remaining 10 units. This would require 3 browser windows, one window for each group of 10 units and one window for all 20.

You must enter the IP addresses of all the slaves into the fields on this page.

MWEB Operation – Connection Status

The MWEB Master communicates to the SERNET slaves to retrieve events as they occur via Ethernet communications. The SER^{NET} slave units initiate continuous communications to the MWEB Master.
The colored annunciator box around the device number indicates:

- White – a connection not yet attempted.
- Green – a slave is connected
- Red – the slave did not connect within the initial 2 minutes
- Orange – a SER^{NET} that was once connected, has gone off-line and is no longer communicating to the master SER^{NET}. The MWEB master will continue to reconnect to this unit every 15 seconds

Warning: When using Combined SER MWEB:
ALL SER^{NET} units must have the same firmware revision for proper operation.

TCP/IP Port:
All units in the network must have the same TCP/IP Port number. The default is 61000.

To change the port number:
Disable the Master.
Log on to each unit and change the port number.
Re-enable the Master.

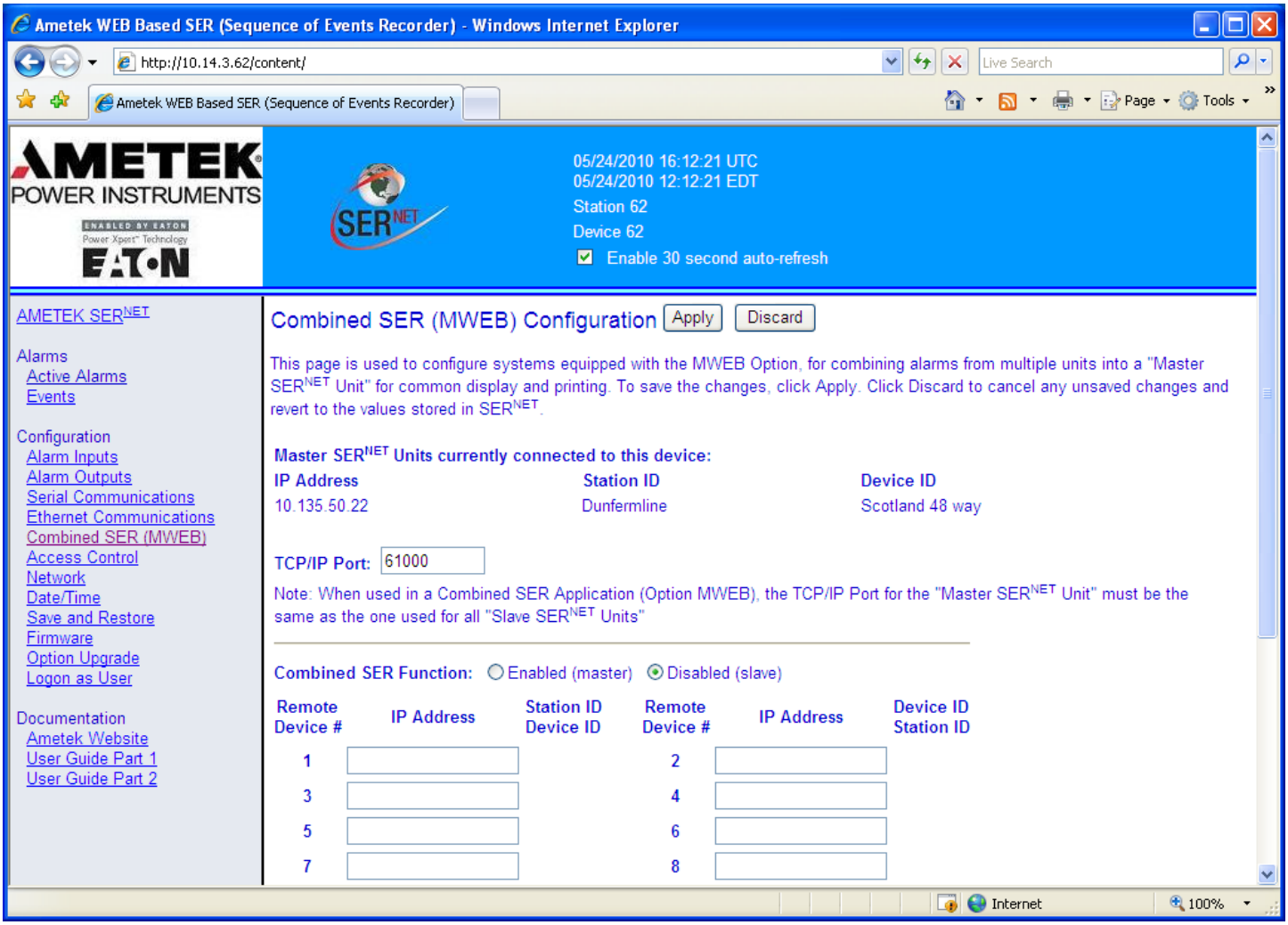


Figure 3–17 Combined SER (MWEB) Configuration Page

Combined SER (MWEB) Application Notes

Alarm Acknowledgement

Alarms can be acknowledged at either the master or slave unit. In the case where alarms are acknowledged at a master but the slave is connected to more than 1 master, the stored event indicates where the event was acknowledged.

For example: In a network where a slave has two masters, i.e. Master 1 with Slave 1 & ***2*** and Master 2 with Slave ***2*** & 3, alarm acknowledgement works as follows.

Alarm Events Acknowledged at Master 1:

- Master 1: Remote Alarm Acknowledged
- Master 2: Alarm Acknowledged at Remote Master
- Slave 2: Alarm Acknowledged at Master

At Slave 2 (which has 2 Masters):

- Master 1: Alarm Acknowledged at Remote Site
- Master 2: Alarm Acknowledged at Remote Site
- Slave 2: Alarm Acknowledged

Event Overload and/or Missing Events

In the case of an extremely high number of events, there may be a rare case where events are missing from the log or the log overflows. If this occurs, an event, “SER Buffer Overflow” is reported. Typically this may occur only after sustaining approximately 80 or more events/second for several minutes and beyond with 35 or more inputs.

An invalid IP address or an off-line slave should be removed from the MWEB configuration as it can degrade the master’s performance.

The following Use Cases offer possible scenarios for MWEB and the effect on Modbus Alarm Points.

Use Case 1: MWEB is started and all slaves are present and connect immediately. The Modbus Map is locked in as displayed below on the MWEB page. The alarm points for Modbus in this case will always be sent in 9 registers (144/16).

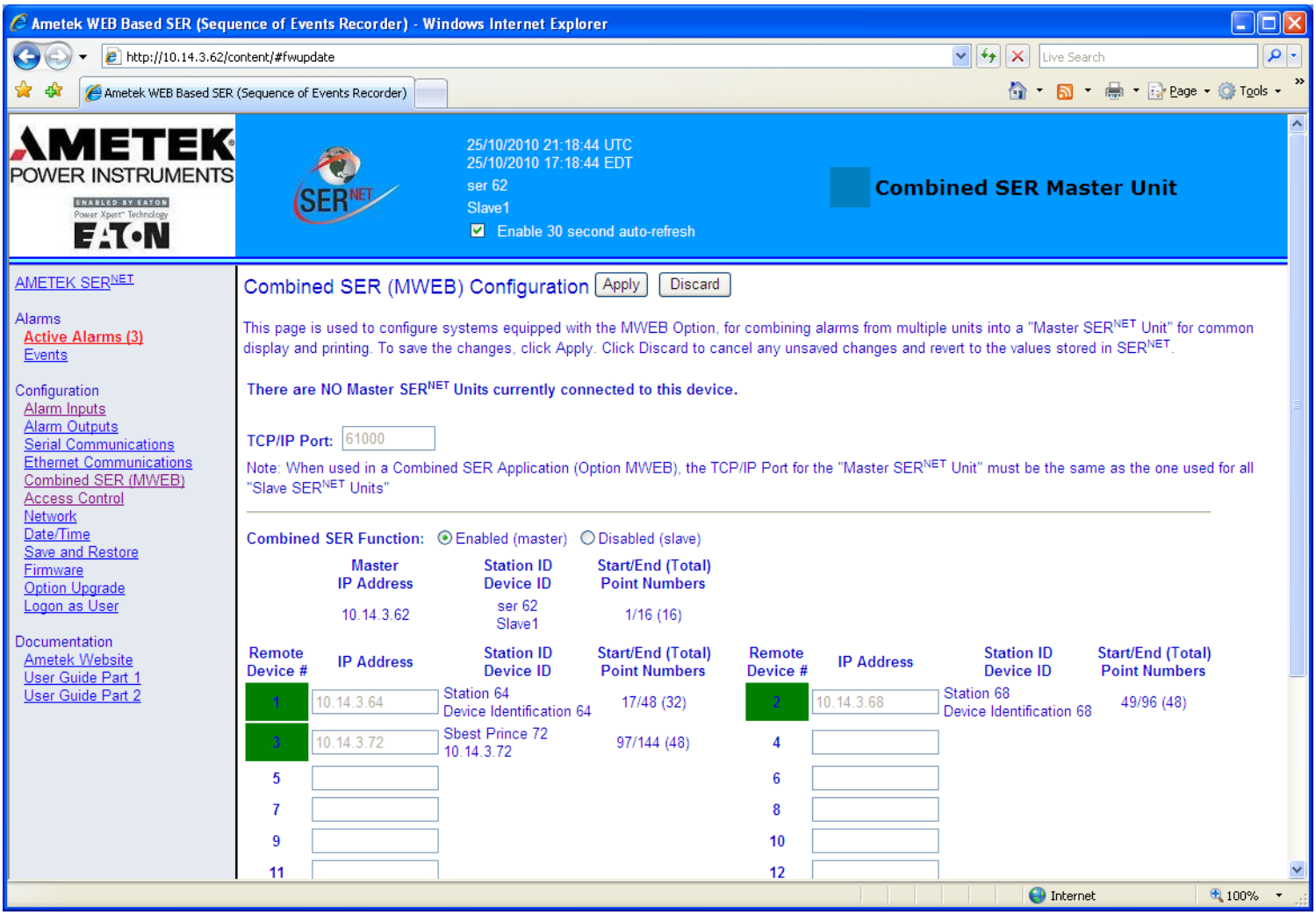


Figure 3–18 Combined SER (MWEB) Use Case #1

Use Case 2. MWEB is started and all slaves are present and connect immediately. Some time after the initial connection to all slaves, one of the Slaves is powered off. In this case the Modbus map remains fixed as it was after initial connection. (alarm points for Modbus will remain at 9 registers). **Once it has been detected that a slave has gone off-line, the alarm points for this unit will be forced to all zeros.** The MWEB display will indicate a SER^{NET} is off-line by displaying the remote Device # in an Orange background as follows:

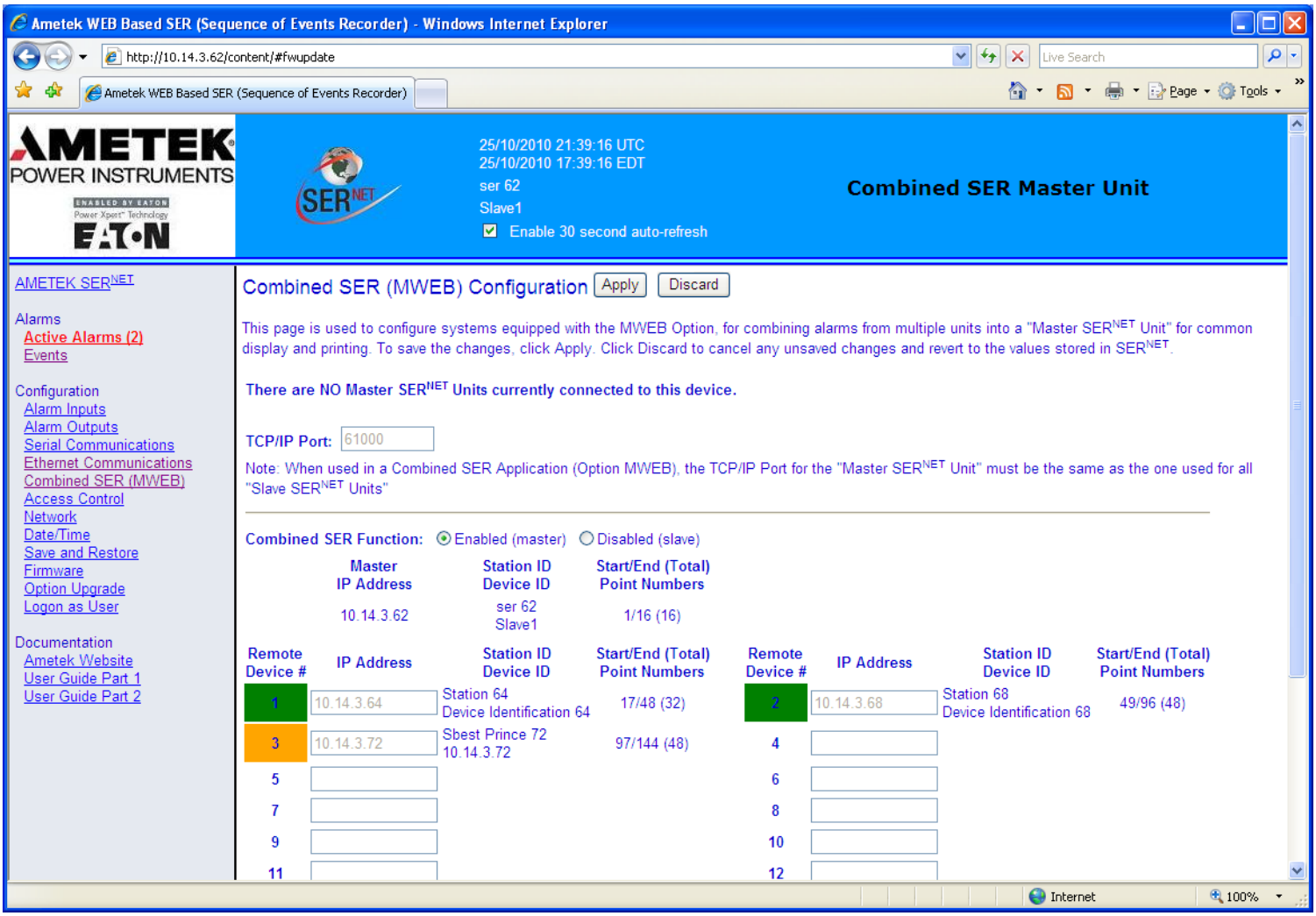


Figure 3–19 Combined SER (MWEB) Use Case #2

When a Slave goes Off-line, the MWEB software does not detect this immediately. The logic in detecting that a slave has gone Off-line is as follows.

- MWEB master expects to receive a message from each slave (containing its LED states) within 120 seconds
- If MWEB has not received this message within 130 seconds then a special request is sent to the slave
- If the Slave does not respond to the request within 30 seconds, it is assumed the slave is Off-line and then; its LED states are cleared, the socket connection is closed, and its state goes to Off-line as shown by the orange background.
  This process can take up to 2.6 minutes. **During this time, the Modbus data sent for**

alarms will equal the last valid state and these will not change to 0's until the unit is declared Off-line. (as indicated with the Orange background on the MWEB page). Additionally an Event "Slave at xxx.xxx.xxx.xxx no longer communicating" will be logged.

- Once a slave is in the Off-line state, every 15 seconds an attempt will be made to re-connect to this unit. If it comes back on-line it will pick up just where it left off, the background for this slave will return to green and an event, "Connected to remote device at xxx.xxx.xxx.xxx" will be logged.

Use Case 3: MWEB started up and 3 of the four slaves were connected within the first 2 minutes of enabling MWEB. The Modbus Map is locked in as displayed below on the MWEB page. The alarm points for Modbus in this case will always be sent in 9 registers (144/16). **The red background indicates that this unit was not found and it is important to note, that NO further attempt will be made to connect to this unit, unless MWEB is disabled and then re-enabled.** This is a change from the way MWEB worked in version 1.01.

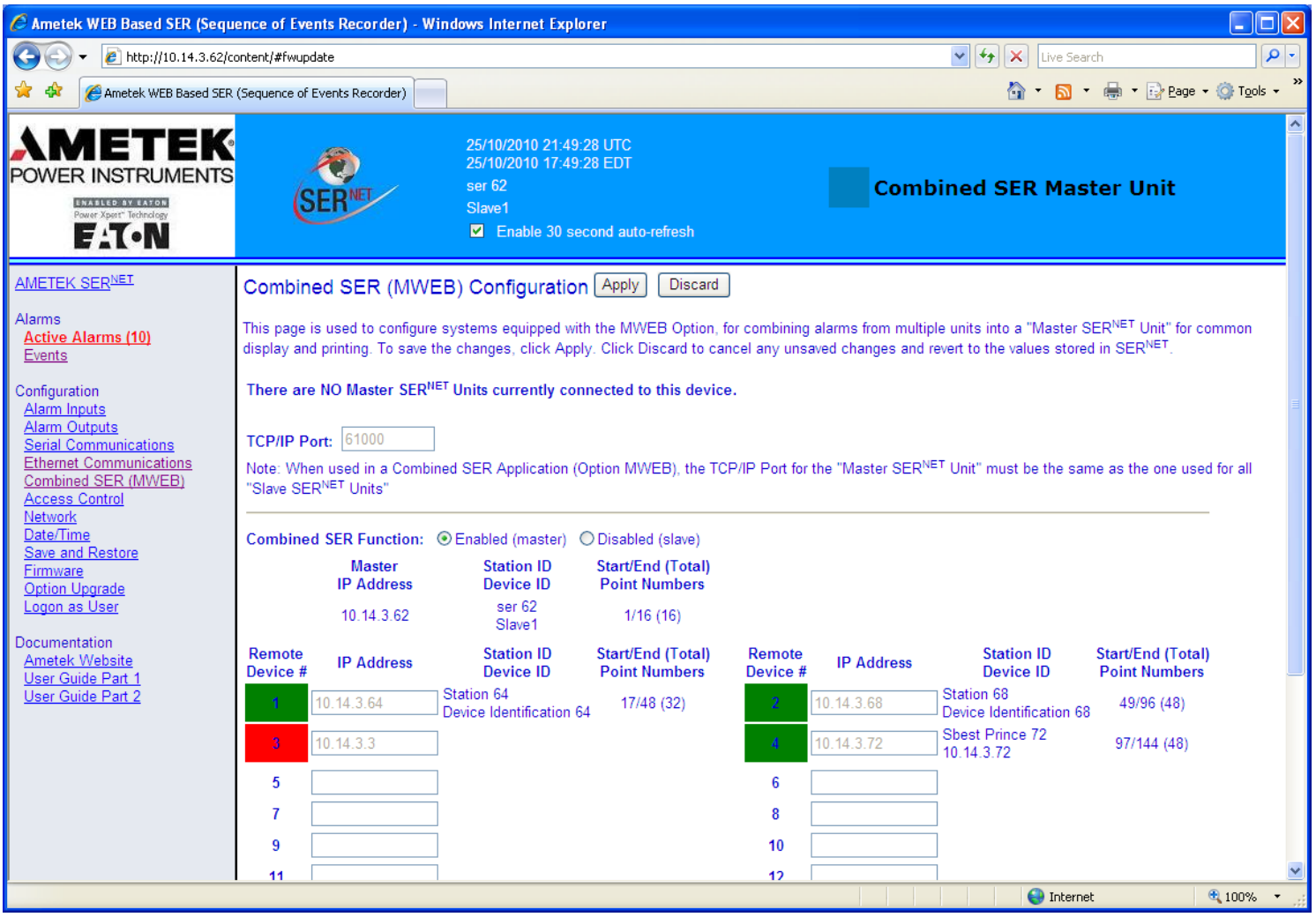


Figure 3–20 Combined SER (MWEB) Use Case #3

Use Case 4: MWEB started up and 3 of the four slaves were connected within the first 2 minutes of enabling MWEB, so all their points are set for the Modbus Map. Some time after the initial 2 minutes, slave 4 goes down. Since it is already included in the Modbus Map it will continue to be represented in the Modbus Alarms. BUT its LED states will be forced to all 0's. And no more events will be sent for this unit as it has been turned off. This Slave is now in the "Off-Line" state represented by an Orange background.

Slave devices with the red background have a state of "Not Connected" and will never be included in the Modbus map.

Additionally, connection to it will not even be attempted again (after the first 2 minutes of enabling MWEB). (Note no point information is displayed for them).

Note: when a Slave goes Off-line, the MWEB software does not detect this immediately. The logic in detecting that a slave has gone Off-line is as follows.

- MWEB software expects to receive a message from each slave (containing it's LED states) every 120 seconds
- If MWEB has not received this message within 130 seconds then a special request is sent to the slave
- If the Slave does not respond to the request within 30 seconds, it is assumed the slave is Off-line and then; its Led states are cleared, the socket connection is closed, and its state goes to Off-line as shown by the orange background.
  This process can take up to 2.6 minutes. **During this time the Modbus data sent for alarms will equal the last valid state and these will not change to 0's until the unit is declared Off-line**. (as indicated with the Orange background on the MWEB page). Additionally an Event "Slave at xxx.xxx.xxx.xxx no longer communicating" will be logged.
- Once a slave is in the Off-line state, every 15 seconds an attempt will be made to re-connect to this unit. If it comes back on-line it will pick up just where it left off, the background for this slave will return to green and an event, "Connected to remote device at 10.14.3.72" will be logged.

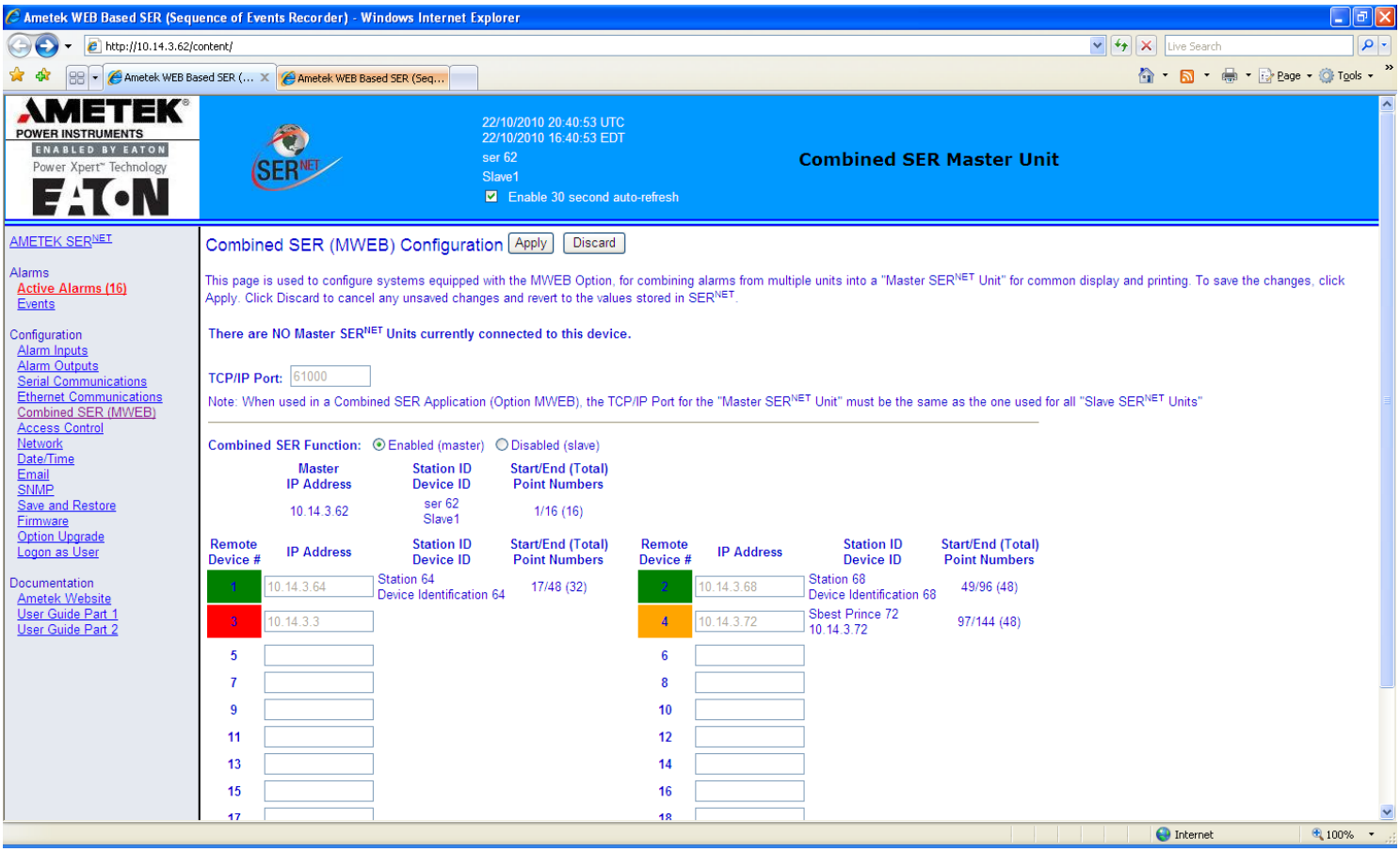


Figure 3–21 Combined SER (MWEB) Use Case #4

Additional notes:

Immediately after MWEB has been enabled, you will see that the starting point numbers will all be initialized to zero and after all connections possible are made, the page will contain the starting point numbers. Note that during this time, neither the External Serial Communication nor the Ethernet Communications will operate. After the communications has been established they will start automatically.

Access Control Configuration

Access control is available to Administrators only. As shown in the following figure, the SER^{NET} is equipped with built-in security to prevent unauthorized access to network configuration parameters, firmware upgrades and other critical settings. This page is where the system administrator sets up user passwords and network configuration such as SNMP and Modbus access and port numbers. As with most password fields, you will only see asterisks as you type in your password.

User and Admin authority are detailed below (respectively):

User Account can:

- View Active Alarms
- View Event Logs
- View Configuration Details
- Sort and Filter Events for viewing purposes
- Export events via csv download
- Print events

Admin Account can:

- Include all of the 'User' functions above
- Change configuration details (anything with an 'Apply' button)
- Set time and date
- Acknowledge Alarms
- Erase the Event Log
- Enable or Disable an alarm
- Change Passwords
- Save and Restore Configuration
- Firmware Upgrade
- Option Upgrade

Trusted IPs/hostnames

To add another level of security to your network, select the appropriate checkboxes if you wish to restrict IP/hostnames for either SNMP or Modbus. Once checked, the traffic to the port will be restricted, allowing access to only those addresses/hostnames that you entered into the trusted field. This works like a firewall. You enter a semi-colon separated list of addresses or hostnames into the trusted field.

Ports

All units in the network must have the same port number. The default port numbers are displayed in their respective fields.

HTTPS

HTTPS requires users to select the secure web log on. You need to identify the specific port address used for this secure connection.

Note: When HTTPS is enabled, you must precede the web browser url address by HTTPS://iIP Address, instead of HTTP://IP Address.

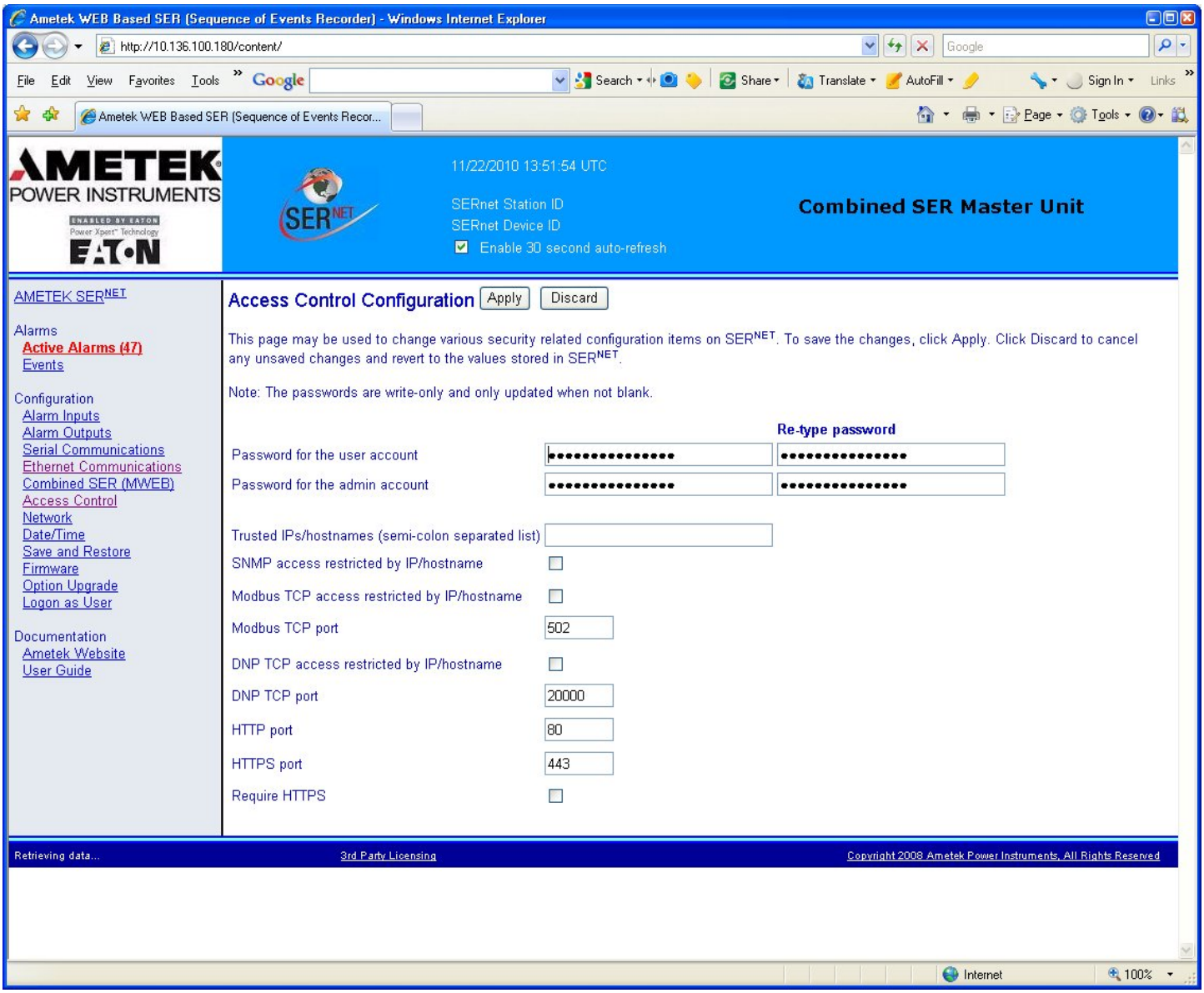


Figure 3–22 Access Control Configuration Page

Network Configuration

This page allows the administrator to configure the network settings. Refer to the following figure. Here you can change your IP address. All units in the network must have a unique IP address. The network administrator configures the network & gateway information according to your location.

If you enable DHCP, you must enter the DNS servers (Nameserver) and the domain into the appropriate fields.

Notice the Ping test field and button at the bottom. If you suspect a unit is not responding or question its connectivity, type its IP address into this field and click the *Test* button. The SER^{NET} will ping the requested unit. The results will be displayed in a new Web browser window.

The standard authentication method used is called 'Digest' which encrypts the log-in information to the unit. In some applications where you have difficulty logging into the SER^{NET}, you may need to switch the authentication method to 'basic'.

Note: After switching the authentication method to 'basic', the units username and password will be reset to the defaults.

After all settings have been made, click the Apply button for those changes to take effect. If you wish to clear all fields to start over, click the Discard button. The "Reboot SER^{NET}" button is available if you wish to restart the system. If using NTP, you must have the Gateway configured properly for NTP to synchronize to its server.

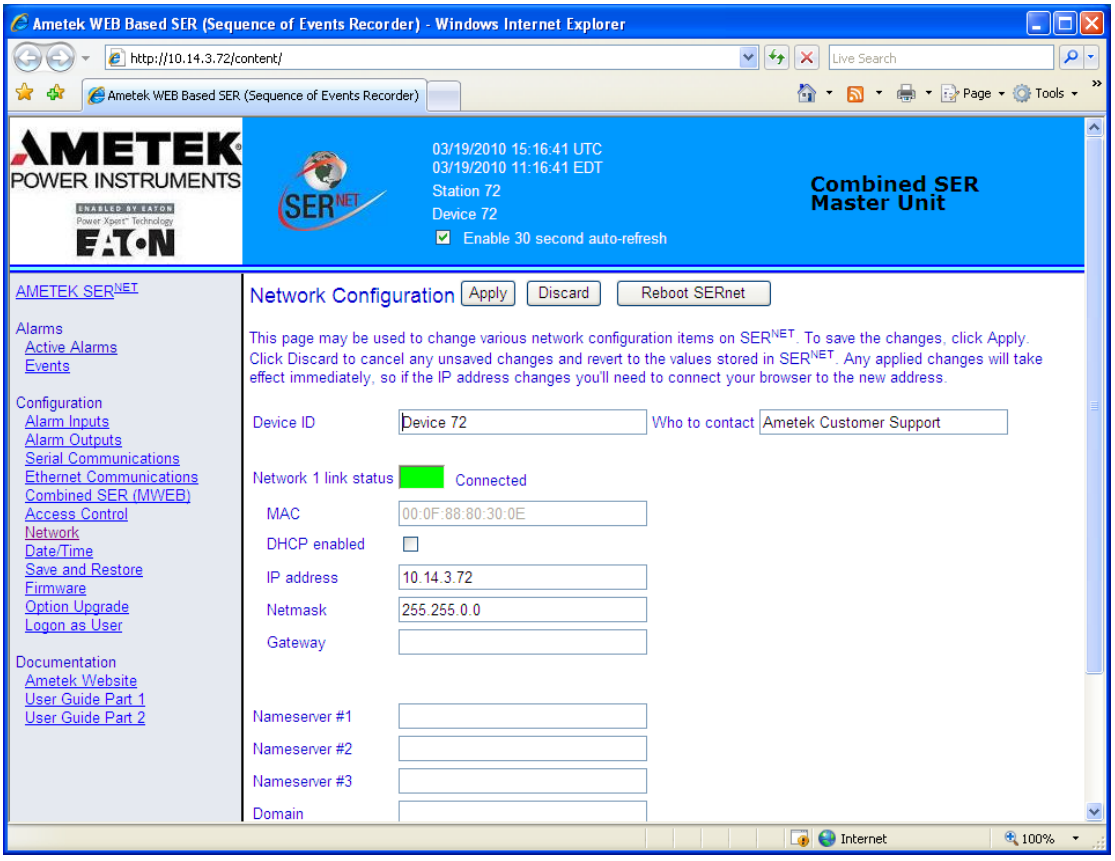


Figure 3–23 Network Configuration Page

Date / Time Configuration

The SER^{NET} date and time can be synchronized to an external time source using IRIG-B, NTP, 1588 or another SER^{NET} unit via RS-485 serial time sync. You can configure multiple time sources for redundancy with in case your primary source loses time synchronization. When using multiple time sources, the system will first synchronize to IRIG-B followed by NTP or 1588. There is an internal crystal to maintain time when no external time sync is provided.

IRIG-B Time Source

IRIG-B is the primary time source. IRIG-B does not require any configuration other than selecting either the modulated or demodulated mode (Fig. 2–11). Once connected to a suitable time source, the IRIG-B time sync status will be noted in red as 'IRIG-B signal detected'.
Note: IRIG-B date does not include the year. If the year is incorrect, you should initially set the year by selecting either "Set Date/Time from PC Clock" or "Set Date/Time Manually" as shown in Figure 3–24 (2nd & 3rd radio buttons under Alternate Time Source).

External Serial Time Sync

A SER^{NET} unit connected to the primary time source can be designated as a 'Master' for sharing the time synchronization signal with up to 24 SER^{NET} units designated as 'Slave'. This is used in cases where you only want to connect IRIG-B to just one unit instead of all units. Or, it can be used when you are not using any external time sync but want to maintain the same time clock amongst all units. Refer to Figure 2-12a and 2-12b for the RS-485 time sync interconnections.
Note: This is not to be confused with the MWEB Master/Slave arrangement. The MWEB connection does not provide time sync between units.

NTP Time Sync

NTP configuration will allow up to three NTP timeservers at different IP addresses. Preference will be given to the best NTP time source and will automatically switch to one of the other NTP timeservers when a signal drops out. Note: You cannot use NTP and IEEE 1588 at the same time.

IEEE 1588 Time Sync

IEEE 1588 configuration requires you to enter the IP address of the master clock. Once connected to a suitable time source, the IEEE 1588 time sync status will be noted in red as 'Synching'.
Note: You cannot use NTP and IEEE 1588 at the same time.

Manual Time Set

When external time synchronization is not used, the SER^{NET} can be configured with the PC time and date or any time and date you enter.

The SER^{NET} has built-in diagnostics to check the time synchronization continuously and every hour, it will be noted in the Event Log. If you wish to remove this hourly time synchronization event, select the option to 'Suppress Hourly Time Sync'.

At the bottom of the page are the fields for setting the date/time format (mm/dd/yyyy) and for choosing your time zone.

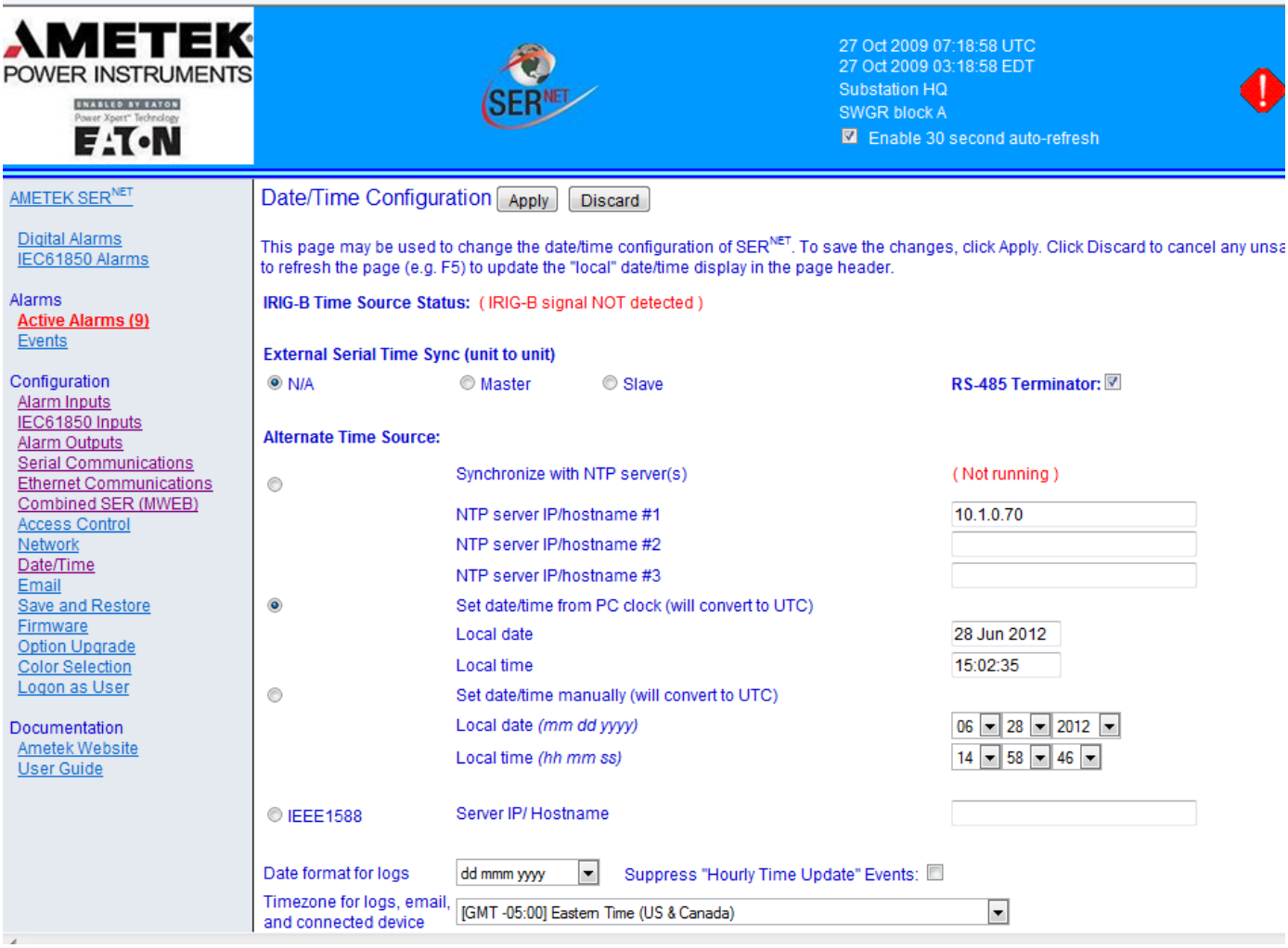


Figure 3–24 Date & Time Configuration Page

Email Configuration

The SER^{NET} can transmit any alarm to three separate email recipients. All alarms or specific ones can be used to trigger an email. The alarm email will include the input number, time and date of alarm and the alarm legend configured in the unit. The frequency of emails can be configured to send them out as soon as an alarm occurs or batch them up at specified intervals.

The SMTP Server IP address or host name needs to be entered based on whatever email system you are using. You must include your username and password that is used for this system. Consult your IT administrator if unsure of the settings. After configuring the SMTP selections, you can test the settings by pressing the 'Test SMTP Server Connection'.

Enter the recipient email address and the frequency of how often the emails will be sent. The frequency can be configured as '0' which is immediately after an alarm or in hourly increments from 1 to 24. When a selection of 1-24 is used, the clock will start at the moment it is configured. Example: If the user selects 12 (for 12 hour increments) and configures it at 8:00AM, they will receive emails at 8:00AM and 8:00PM.

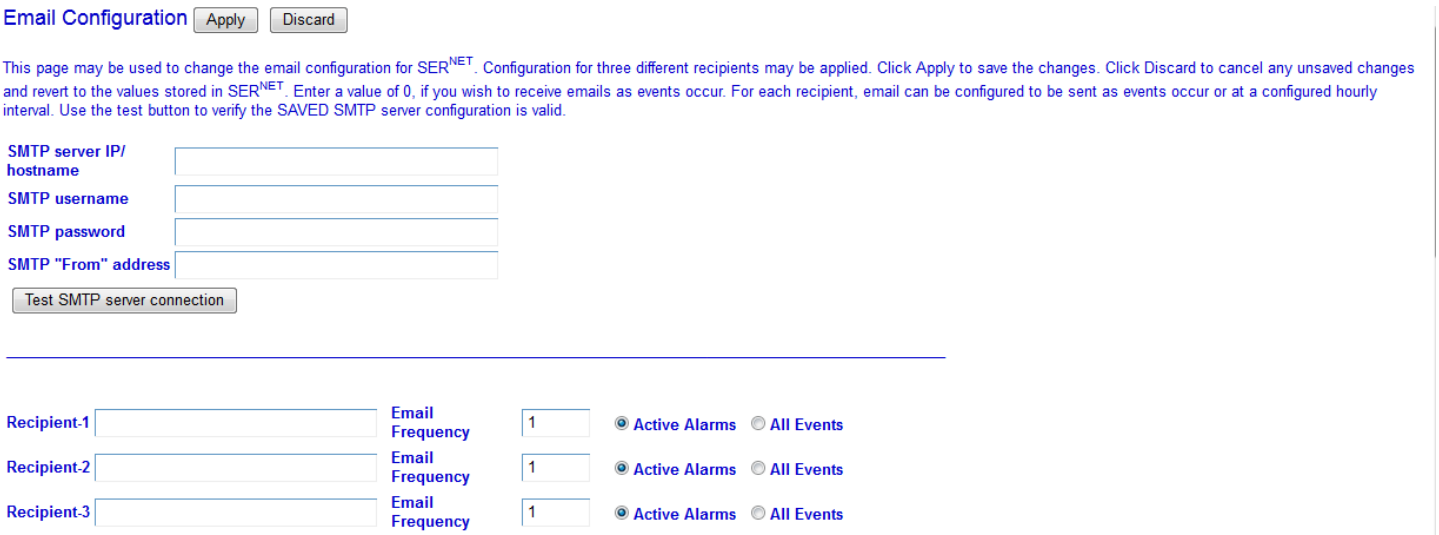
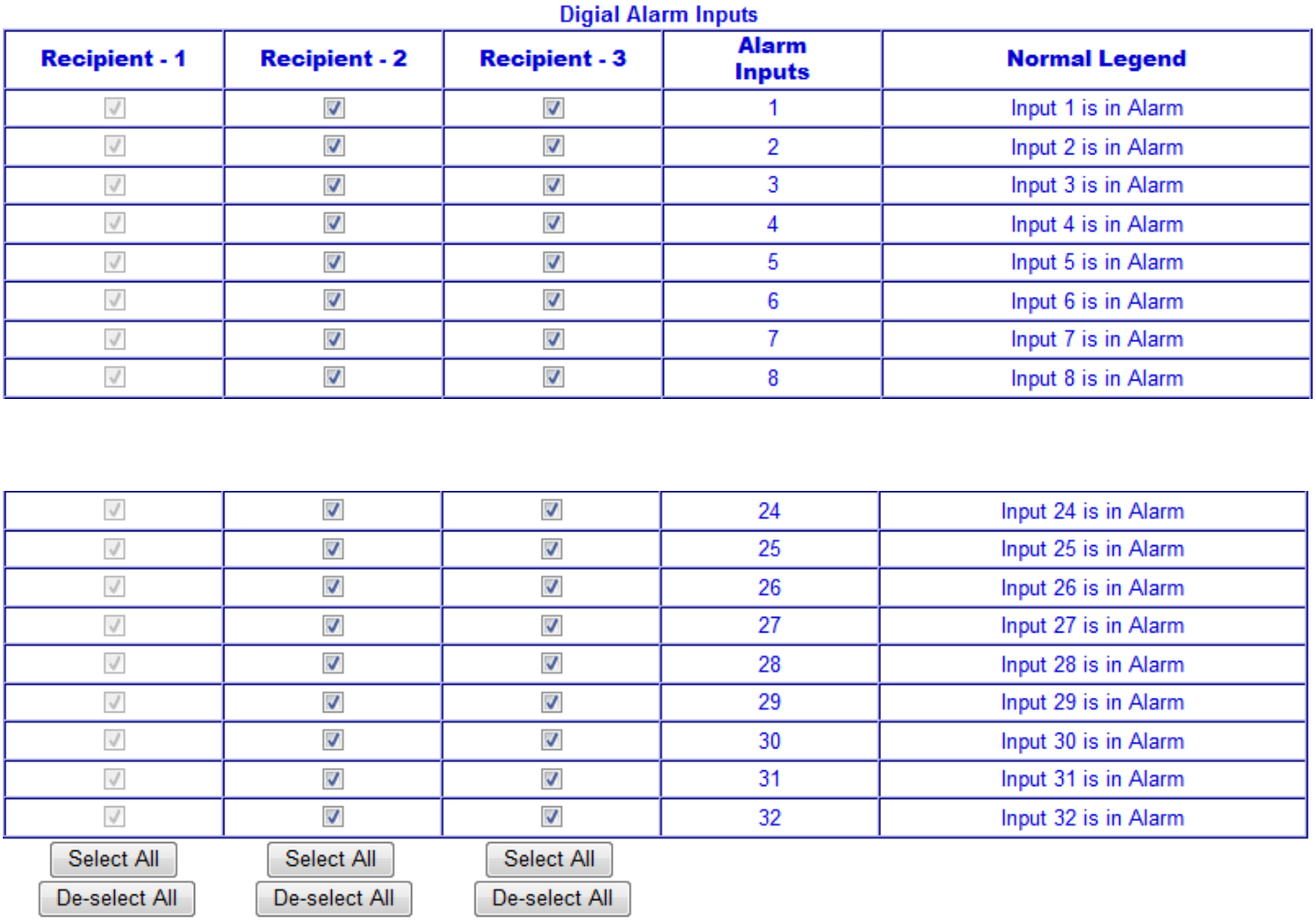


Figure 3–25A Email Configuration Page

Active Alarms: When this is used, the email will only contain the selected inputs that are in the Alarm State at the moment the email is generated. If none of the inputs selected are in alarm, no email will be generated. For example, if all inputs were selected and the interval was 24, then the email will include any inputs that were in the alarm state at the moment the 24 hour email is generated. (This time is based when you first configure the unit) If the frequency is set at 0, an email will be generated after the selected input goes into alarm. (Note: A 15 second filter is included in case the input returns to normal before the 15 seconds is up.)

All Events: When this is selected, the email will contain all changes of state for the selected inputs starting at the beginning of the time interval to the end of the time interval. For example, if Input #7 was selected and the frequency of emails was 24, the email will include all alarm and return to normal timestamps of Input 7 that occurred in the 24 hour period.

A list of Digital Alarm Inputs and IEC 61850 Inputs (if equipped) will be shown along with checkboxes for each email recipient. Check the alarms that will trigger an email for each one of the recipient email addresses entered above. Use the ‘Select All’ and ‘De-select All’ buttons speed up the entry of inputs.



Digial Alarm Inputs

Recipient - 1	Recipient - 2	Recipient - 3	Alarm Inputs	Normal Legend
☑	☑	☑	1	Input 1 is in Alarm
☑	☑	☑	2	Input 2 is in Alarm
☑	☑	☑	3	Input 3 is in Alarm
☑	☑	☑	4	Input 4 is in Alarm
☑	☑	☑	5	Input 5 is in Alarm
☑	☑	☑	6	Input 6 is in Alarm
☑	☑	☑	7	Input 7 is in Alarm
☑	☑	☑	8	Input 8 is in Alarm
☑	☑	☑	24	Input 24 is in Alarm
☑	☑	☑	25	Input 25 is in Alarm
☑	☑	☑	26	Input 26 is in Alarm
☑	☑	☑	27	Input 27 is in Alarm
☑	☑	☑	28	Input 28 is in Alarm
☑	☑	☑	29	Input 29 is in Alarm
☑	☑	☑	30	Input 30 is in Alarm
☑	☑	☑	31	Input 31 is in Alarm
☑	☑	☑	32	Input 32 is in Alarm

Select All | Select All | Select All

De-select All | De-select All | De-select All

Figure 3–25B Email Configuration Page

Sample Email Format:

```
------------------------------------------------------------
Station ID      = Juniper West Substation
Device ID       = SERnet IP: 10.41.23.456
Time Interval   = 08/22/2012  11:51:07  -  08/22/2012  12:51:07
------------------------------------------------------------

Point           = 41
Description     = Input 41 has returned to Normal
Normal          = 08/22/2012  11:58:21.301
------------------------------------------------------------
Point           = 23
Description     = Input 23 is in Alarm
Alarm          = 08/22/2012  11:59:21.720
```

Save and Restore Configuration

This page provides a way for you to save the unit's configuration to an XML file. The advantage to this is if for whatever reason you need to reload the SER^{NET} configuration at a later date, you'll have the configuration file saved already. Simply browse to the file on your PC and restore the configuration file to the unit.

Note: it is strongly advised to have a copy of each SER^{NET} configuration file saved at all times. After you make changes, save a new copy by clicking on the *Save Configuration* button.

To restore a configuration (refer to Figure 3–26):

Click the *Browse* button.

From the choose file dialog, select the configuration file to be downloaded to SER^{NET}.

Click Open and a message box will pop up asking you to confirm your action. Click Ok.

Your SER^{NET} unit will be re-configured with the saved file, including all Alarm Inputs and Outputs.

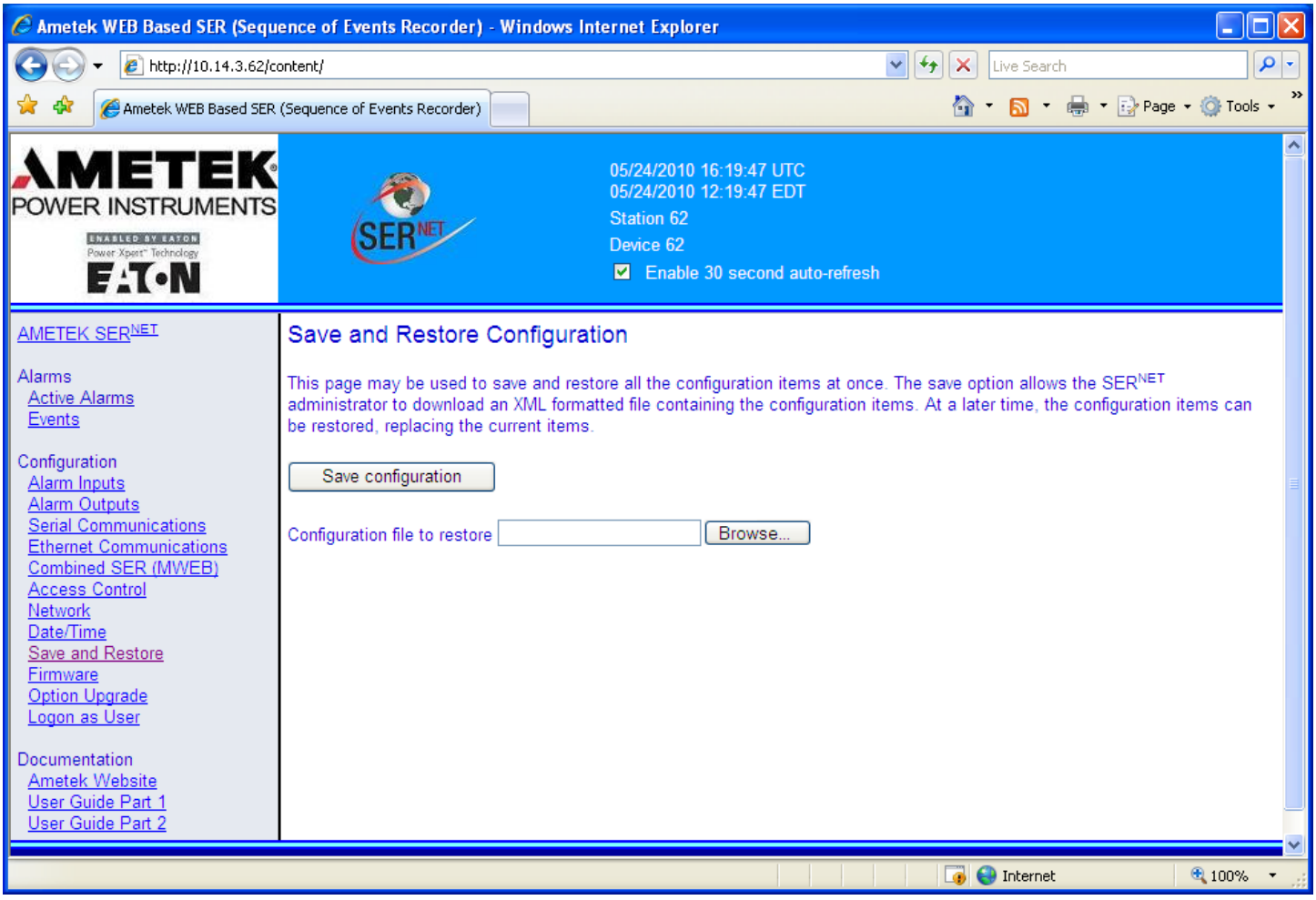


Figure 3–26 Save and Restore Configuration Page

Firmware Configuration

The current version number of Software/Firmware installed on your unit is provided on the SER^{NET} Home Page, as shown in Figure 3-27a.

If a new version of the SER^{NET} firmware is available, this page is where you upload the new file. See the following figures. Simply browse for the file on your PC and after you choose the new file, it will begin uploading after your confirmation. The original system configuration will be restored after a firmware upgrade, but it is always good practice to save a copy of this configuration prior to the firmware upgrade using the 'Save and Restore' function.

Caution: during a firmware update, do not close the browser window or power down the unit. Doing so will cancel the upload process and corrupt the firmware.

As seen in Figure 3–27b, during the firmware update process, the file status progress bar will indicate the status of the update.

Green status (Finished or No Update) – update successful.

Yellow status – potential red status event with one of the module updates, or the main board download may have exceeded the 5 minutes allotted to its download. Either way, it's more of an alert than necessarily an error for that particular update.

Red status (File Error, or Hardware Error) – may be one of the following:
the file that you were trying to download is not correct
the file could be corrupted
there was a hardware problem in attempting to erase, or write to the flash

Any status other than green should be reported to your AMETEK representative.

After the firmware is upgraded, you will be prompted to re-boot the SER^{NET}. This can be done automatically by selecting the checkbox 'Reboot when complete' before you start the upgrade process.

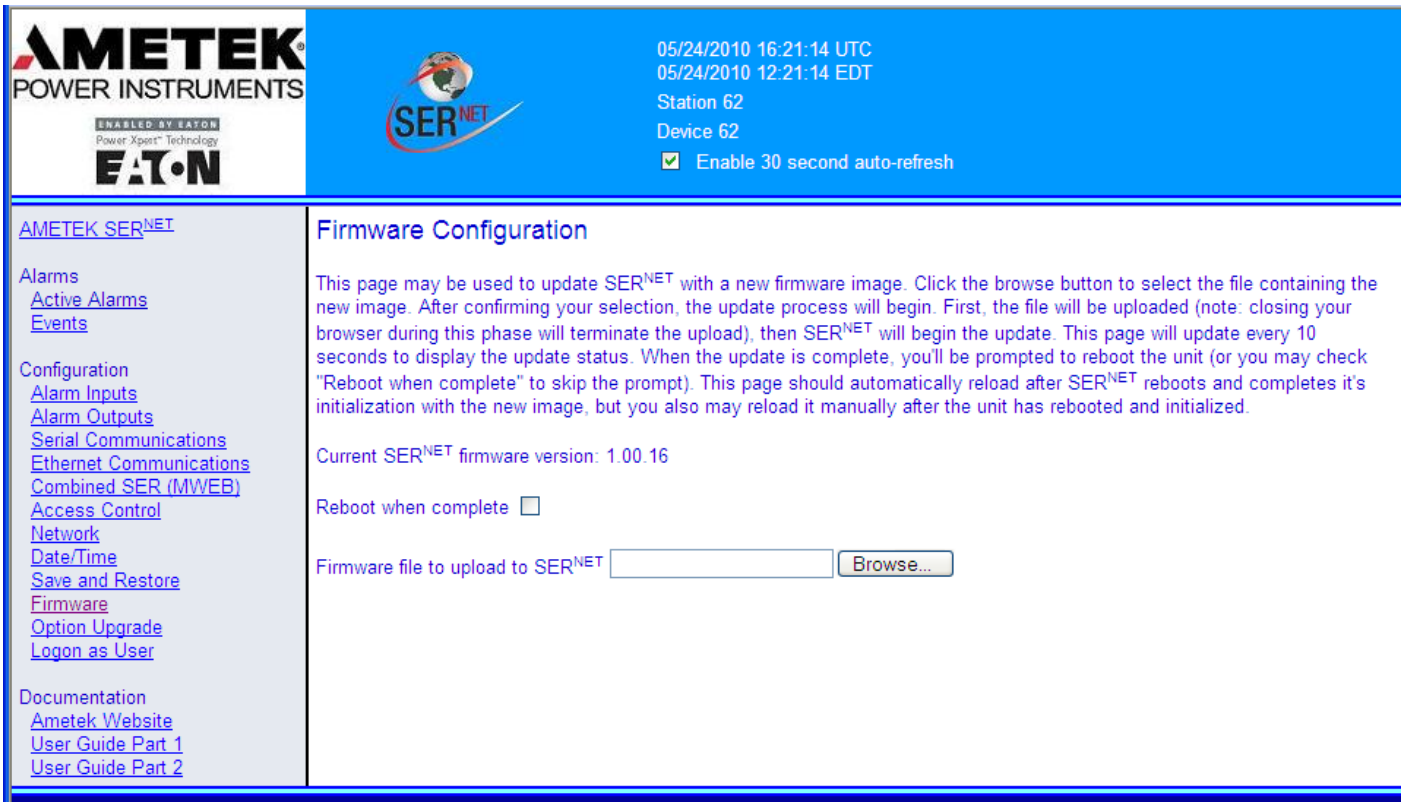


Figure 3–27a Firmware Configuration Page

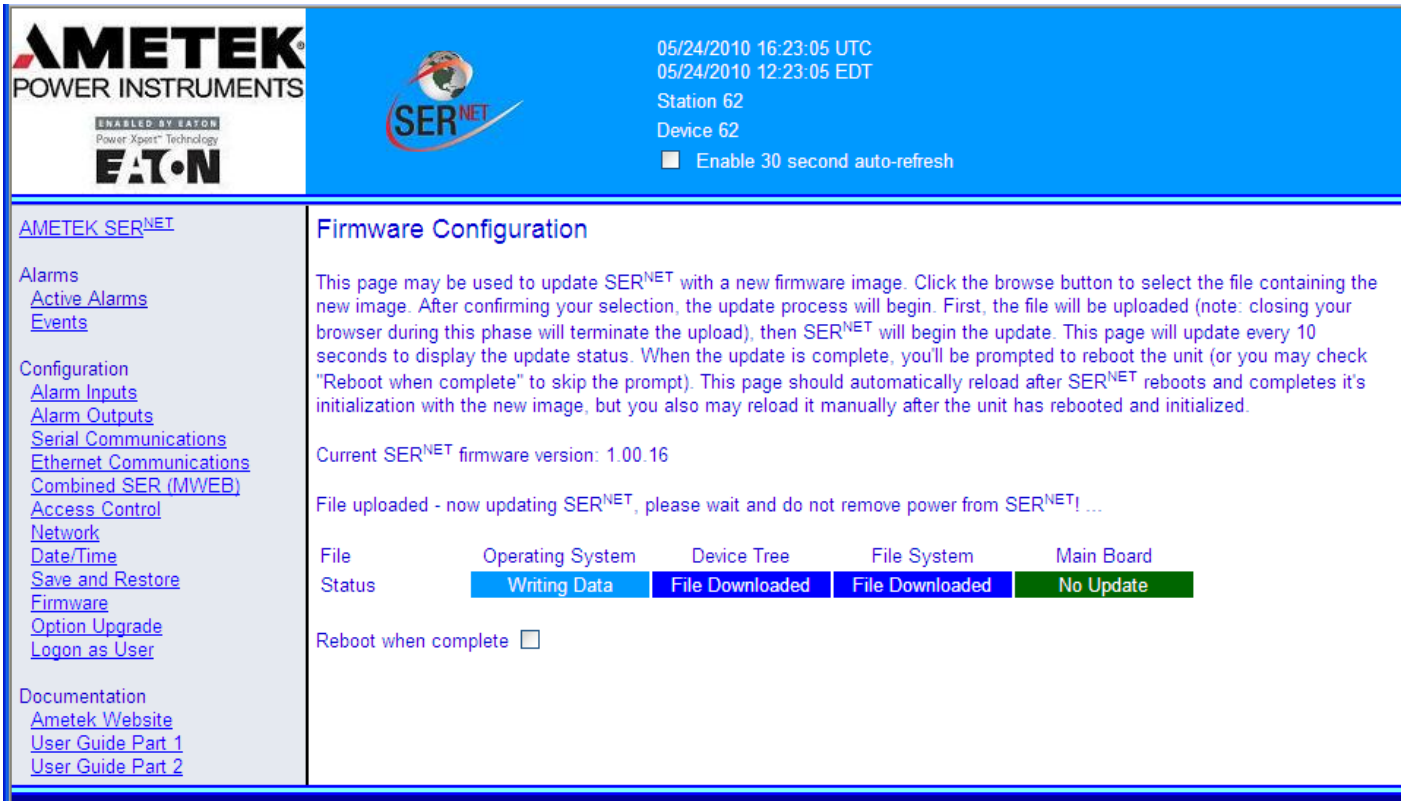


Figure 3–27b Firmware Configuration Page After Update

Option Upgrade

SER^{NET} can be upgraded in the field. The primary purpose of this function is to enable various options that were not supplied with the original unit. The SER^{NET} home page will identify the model number of your SER^{NET} unit and the options provided. A description of this model number is shown in Chapter 1. The available options that can be upgraded are:

Option Code	Option	Description
MOD	Modbus Communications	Modbus RTU and Modbus TCP/IP modes
DNP	DNP Communications	Serial and Ethernet modes
MWEB		Single web browser displays alarms from up to 24 SER^{NET} Units via Ethernet LAN
IEC61850	IEC61850 Communications	The IEC 61850 alarms received by the SER^{NET} can be displayed on the WEB Browser Graphic Screen. The IEC 61850 alarms will be merged with the 'digital' contact inputs for one common WEB Browser display using the Active Alarm page and Event Log.

1. Simply call your AMETEK representative to request new options.

a. You will need to know your unique MAC address and which options you desire to upgrade.
b. Your rep. will then give you a unique Upgrade Key specific to the unit you wish to upgrade.

2. This Upgrade Key must be entered exactly as provided.

3. Once you enter the Upgrade Key, click the *Submit Key* button and the unit will display the proposed model configuration.

4. Examine the details and if they are correct, click *Upgrade Unit*.

5. Click the *Yes* button to complete the process, which will reboot the unit.

Note: If an error occurs or perhaps you mistyped a letter, a failure message will appear at the bottom of the page. Carefully retype the Upgrade Key in and click *Submit Key* again. And repeat steps 2–5.

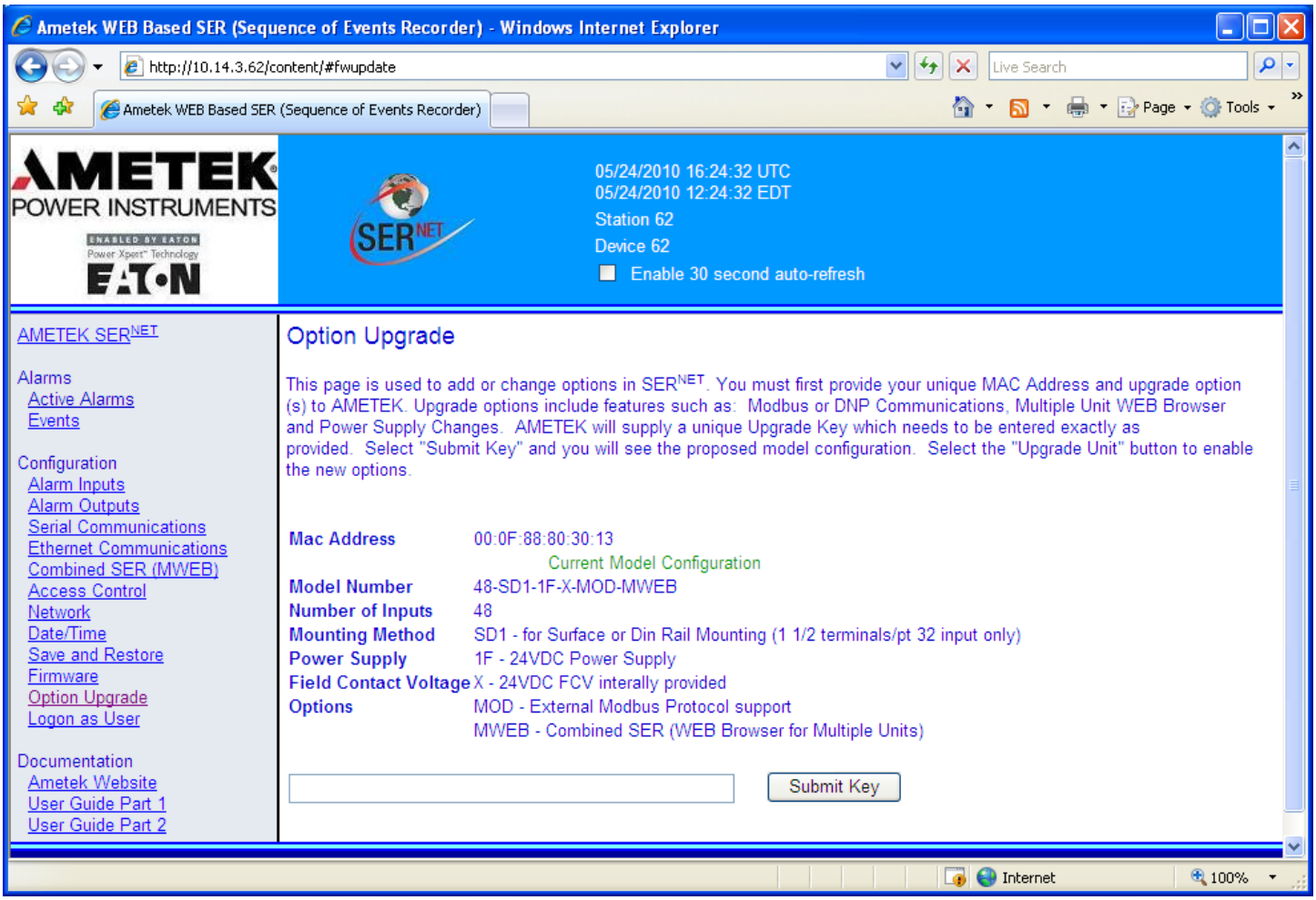


Figure 3–28 Option Upgrade Page

Color Selection

The SER^{NET} can display alarms in several graphical formats which can be selected in the color configuration screen. The Home Page, Active Alarm and Event pages can be color coded for the background and text colors of various events. The configuration page will show the current color selection and provide new selections for background and text colors as applicable.

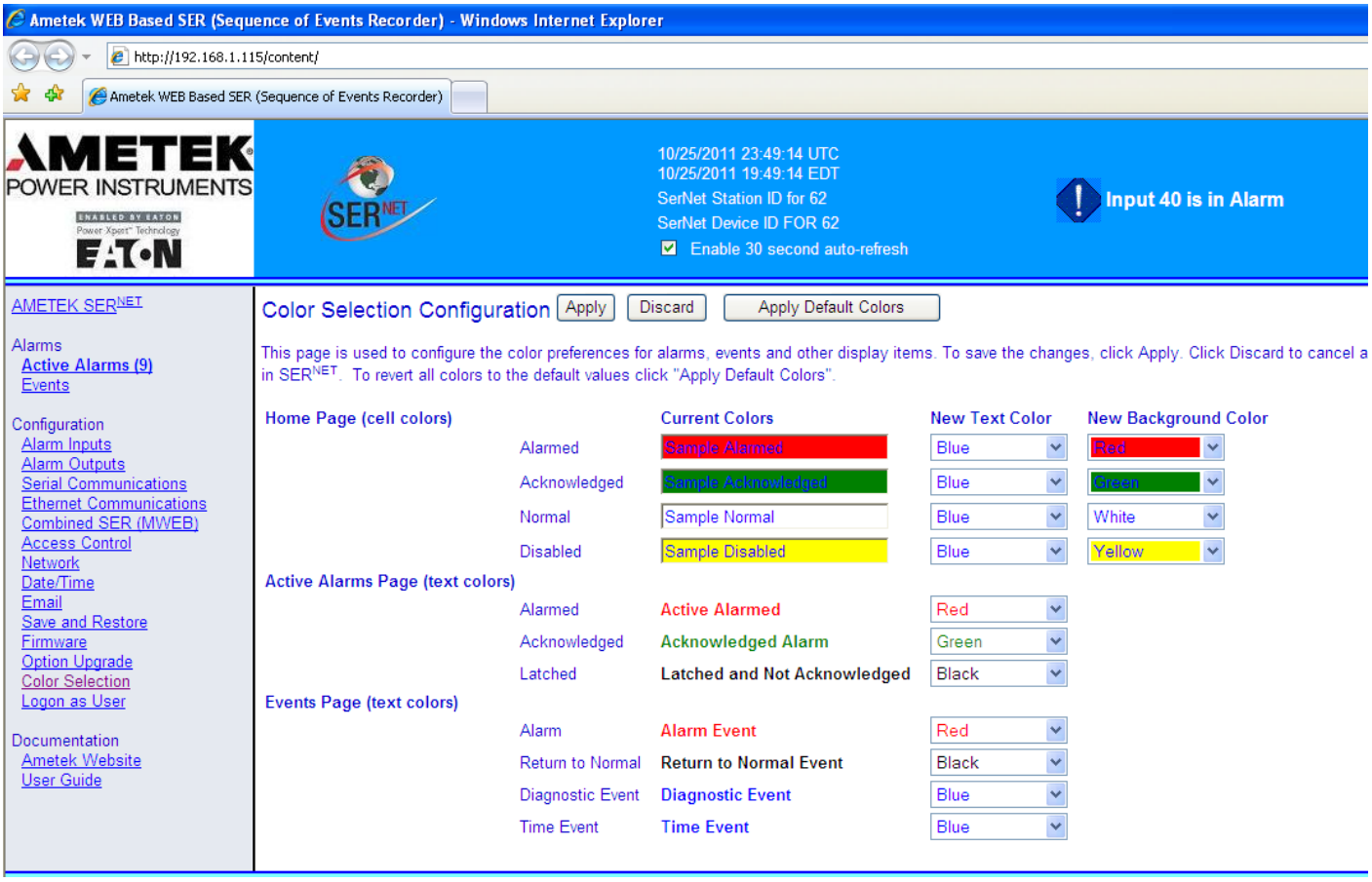


Figure 3–29 Color Selection Page

Logon as User

To switch logon type click this link. If you are logged in as User, it will display *Logon as Admin* and vice versa. Remember, User logon is restricted. You will be prompted with a logon dialog box as shown in Figure 3–1.

Documentation

At the bottom of the side-bar you'll find links to the Ametek Power Instruments Web site, User Guide and MIB files. MIB files are files used to configure SNMP traps.

Chapter 4-Service & Maintenance

Firmware Upgrade *(Firmware Configuration Page)*

Your AMETEK sales rep. will notify you of firmware upgrades. And you can download the new file from their Web site or via e-mail. To upgrade the firmware:

Make sure you are logged in as Administrator.

Click the *Browse* button

From the Choose File dialog box, locate the new firmware file (.tar).

Click Open.

Confirm that you want to upgrade the firmware.

As the system firmware is being upgraded, the status will be displayed detailing each step of the upgrade. You can check the box labeled “Reboot when complete” to have the system automatically reboot after the upgrade is complete.

Real Time Clock (RTC) battery

SER net uses a 3 volt lithium coin cell for maintaining the internal RTC. The expected battery life is as follows:

Unit continually off:	10 years
Unit off 50 % of the time and operating 50% of the time:	19 years

Reset Password & IP Address

If you have forgotten your password or IP address you can reset SER^{NET} while connected to a terminal emulation program and view or change these items. As shown in Figure 4–1, accessible through a small hole is a reset microswitch inside the unit. Typically you would use a straightened paper clip through the hole to press it.

To reset the unit:

Power up the unit and wait 15 seconds after unit is operational.
Press the microswitch with a paper clip. This sets a flag in the database that will take effect upon next reboot.
Power off the unit.
Make sure you have a cable connected from the serial port to your PC before power up.
Open a terminal emulation program, as shown in Figure 4–2 and configure it as follows:
9600 baud, 8 data bits, 1 stop bit, No parity
Power on the unit.

In your terminal program, you will be presented with numbered menu choices to reset the password to default, change the IP address etc. After making the changes, type y for Save & apply all settings. If you have changed the IP address, you need to open the network page in your browser and make sure it reflects what you changed.

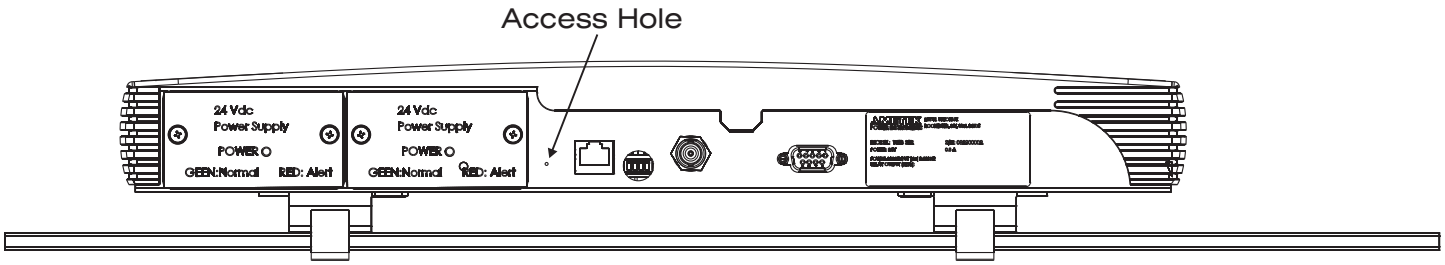


Figure 4–1 Access Hole

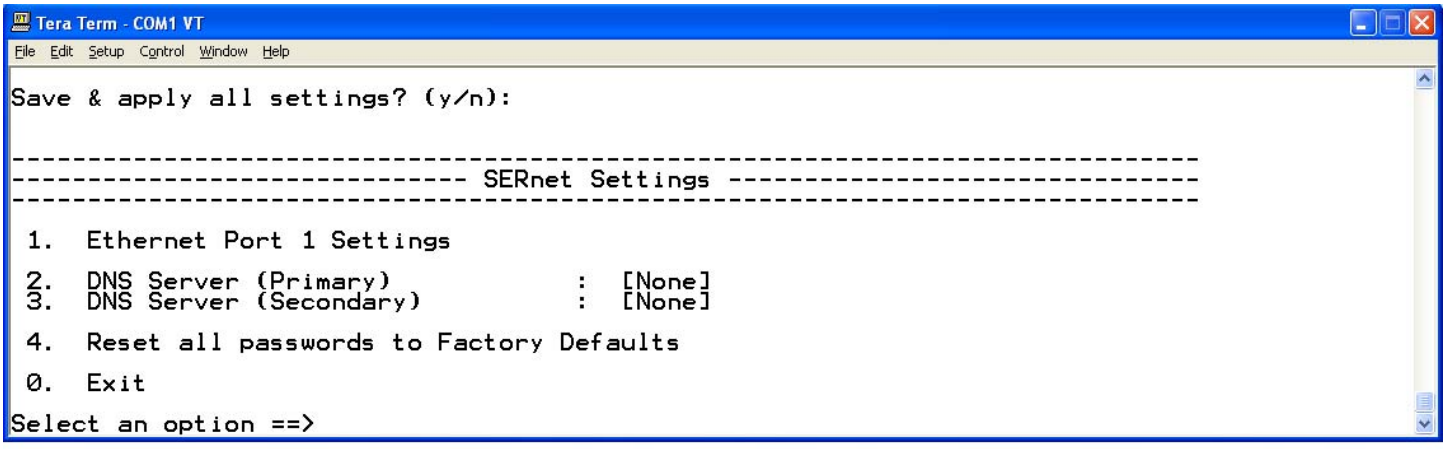


Figure 4–2 Terminal Emulation Program Display

Chapter 5. System Specifications

INPUT

System Capacity

• 16, 32, 48 inputs per unit depending on model

• 3,072 inputs per SER system

Field Contacts

• Normally Open (N.O.) or Normally Closed (N.C.)

• Wetted (voltage supplied) or dry (voltage free) contacts

Field Contact Voltage Range

Models: SD, RK, RK1, SD1, ICR1, RK3, SD3, ICR3

• 20-150 VDC (auto-select)

Models: RK2, SD2, ICR2

• 120 V AC • max 2mA per input

Input Response

• 1 millisecond to 60 seconds

Model: RK2, SD2, ICR2

• 50 milliseconds to 60 seconds
(required to filter the AC input signal)

Contact De-Bounce

• 0-60 seconds

Built-in filter to screen out sub-millisecond contact bounce or noise.
Each Input requires 4 continuous successful samples (at 0.5 msec each) before alarm is captured. Time stamp recorded at first successful sample of the 4. Once an alarm is recorded, it can be configured to eliminate repeat contact bounce lasting 0-60 seconds.

Delete From Scan

Automatic Mode

• Adjustable from 0-255 events per minute. Automatically resets itself

Manual Mode

• Disable any input manually

ALARM LEGENDS

- 32 character alarm legend
- 32 character normal legend

LED INDICATORS

Alarm Status

• One red LED per each input on models SD and RK

• One red alarm LED to indicate on alarm on any of the 48 inputs for models SD2, SD3, RK2 and RK3• Flash upon alarm, steady ON after acknowledged via WEB browser

Power, Status, Time Sync on models SD, SD2, SD3, RK, RK2, and RK3• Green LED for "Normal"

• Red LED for "Abnormal"

OUTPUTS

Alarm Relays

• 2 form C (SPDT) relays, configurable via WEB browser for:

- Common alarm (closes on any alarm)

- Reflash alarm (pulses upon new alarm)

- System watchdog

• Energized or de-energized operation

Relay Ratings

• 24 VDC @ 2.0 amps
• 120 VDC @ 0.4 amps
• 120 VAC @ 2.0 amps

TIME STAMPED ALARMS

• 1 ms time stamp resolution
• 40,000 event storage (per unit)

TIME SYNCHRONIZATION

• IRIG-B

Time sync input (modulated or de-modulated) accurate to +/- 1 ms UTC Time
Modulated or Demodulated, 10K ohm input impedance

• NTP time sync

NTP can have an accuracy up to +/- 1 ms of UTC time when connected to a Quantum 2 NTP Time Server. The NTP time sync is provided via the Ethernet port, which is configured to connect to up to three IP addressable high accuracy GPS clocks installed on the network LAN.

• IEEE 1588 time sync
IEEE 1588 can have an accuracy up to +/- 1 ms of UTC time when connected to a IEEE 1588 Time Server. The IEC1588 time sync is provided via the Ethernet port.

• Master/Slave RS-485 Serial time sync
Master unit with IRIG-B Time Source (or other alternate time sync) can synchronize up to 24 "Slave" units via RS485 (max 4,000 feet). Accuracy to +/- 2 ms of Master Time Source

• Internal Crystal
Accurate to 1 sec/day

COMMUNICATIONS

Serial Port
• RS-232/485 selectable

Protocols
• Modbus RTU

Master Mode
Connect to a maximum of 3 Modbus Slave Devices
Transmit Alarm Status and/or Event with timestamp

Slave Mode
Transmit Alarm Status and/or Event with timestamp

DNP 3.0

Slave Mode
Transmit Alarm Status and/or Event with timestamp

Serial ASCII

Ethernet Port
• 10/100
• DHCP or Fixed IP
•Maximum of 10 simultaneous connections (communication protocols, web browser sessions)
• Modbus TCP/IP, DNP, IEC 61850 Communication Protocols

WEB Server
• Used for configuration of unit
• Graphical and text display of alarms
• Can combine up to 25 units on a single WEB browser (1,200 alarms)
• Sorting and filtering functions

• Acknowledgement of alarms
• Separate screens for active alarms and archived event log
• Email notification
• Export to CSV
• Printing of alarms (auto/manual)
• Multiple levels of security

CONNECTIONS

Field Contacts, Relay Outputs, Power Inputs, Master/Slave Time Sync
• Removable barrier terminal block
12-24 AWG wire, Torque rating 5 lb. in.

Serial Communication Port
9 Pin Female D connector

Ethernet Communication Port
RJ45 connector

IRIG-B Time Synchronization Input
BNC connector

MECHANICAL

Surface Mounting

• Din rail / panel
• 17.8”(452) x 6.8”(172) x 2.3”(58)

19” Rack Mounting

• 1U
• 6.8" (172) Depth

POWER REQUIREMENTS

Internal Power Supplies

24VDC Power Supply
• 24 VDC (19-29 VDC)
AC/DC Power Supply
• 85-288 VAC 50,60 Hz
• 100-300 VDC

Can use 1 supply above or 2 for redundancy / dual power applications
• Hot swappable

Power Requirements	120 Vac, 0.20 A maximum
	240 Vac, 0.10 A maximum

125 Vdc, 0.20 A maximum

24 Vdc, 0.40 A maximum

External Power Supplies

48 VDC Power Supply

• 48 VDC (36-72 VDC)

- Output: 24 VDC (requires internal 24 VDC power supply above)

External Field Contact Voltage Supply

Part Number	Input	Output	# of SER^{NET} Field Contact Inputs
6005-331	100-250VAC/105-300VDC	125 VDC	350
6005-332	90-265VAC/110-350VDC	125 VDC	900

Environment

Operating Temperature Range: -20 to 60 ˚C (-4 to 140 ˚F)

Relative Humidity: 20 – 95 % non-condensing

Storage Temperature Range: -20 to 80 ˚C (-4 to 176 ˚F)

Electrical, Models RK and SD only

Surge Withstand: ANSI C37.90.1 2.5 kV Oscillatory, 4kV Fast Transient

Electrical Fast Transient/Burst Immunity:

IEC 61000-4-4 2kV dc Power, 1kV I/O

Surge Immunity: IEC 61000-4-5 2kV dc Power, 1kV I/O

Radiated RFI Immunity: IEC 61000-4-3 10 V/m

Conducted RFI Immunity: IEC 61000-4-6 3V

Radiated Emissions: CISPR11 Class A

Conducted Emissions: CISPR11 Class A

Radiated Power Frequency Magnetic Field:

IEC 61000-4-8 30 A/m

ESD Effects: IEC 61000-4-2 4kV contact 8kV air

Dielectric Withstand:

FROM (1)	TO (1)	Withstand voltage
Power Input 1	Power Input 2	2000 Vdc
Power Inputs 1 & 2	Earth	2000 Vdc
Power Inputs 1 &2	Relay outputs	3150 Vdc
Power Inputs 1 &2	Field contact Inputs	3150 Vdc
Power Inputs 1 & 2	Digital Communication, except for Ethernet	3150 Vdc
Power Inputs 1 & 2	Ethernet	2000 Vdc
Relay outputs	Earth	1320 Vdc
Relay outputs	Digital Communication, except for Ethernet	2100 Vdc

FROM (1)	TO (1)	Withstand voltage
Relay outputs	Ethernet	1320 Vdc
Field contact inputs	Earth	1320 Vdc
Field contact inputs	Digital Communication	2100 Vdc
Field contact inputs	Ethernet	1320 Vdc

Appendix A MODBUS Data Format

The system has the capability of operating with two distinct data formats: Status Mode (On/Off status) and Event Mode (Alarm Status with Time Stamp). These formats are embedded within Modbus data registers for transmission and reception.

A selection of Modbus function may be used and these vary depending on whether the SER^{NET} is operating as a Modbus master or slave.

Modbus Function	Description	Data Units	Mode
03	Read Holding Registers	Words	Master or Slave
07	Read Exception Status	Bytes	Slave Only
16	Preset Multiple Registers	Words	Master or Slave

A function value of 03 (Read Holding Registers) is set to read alarm data from the system (in slave configuration). Single and multiple register writes are supported. Exception status responses (function 07) and Slave ID (function 17) are also supported. Exception codes for unrecognized received messages are also included.

The Modbus functions are enabled by the software model number and require a key to enable them, which is supplied by Ametek. This may be done prior to delivery or retrofitted in installed systems.

Modbus Operation

The SER^{NET} Modbus operates as a Master or Slave in both Modbus RTU and Modbus TCP/IP modes. The SER^{NET} Modbus port will transmit the ON/OFF Status (called 'Alarms') and the timestamp recorded for every alarm and return to normal occurrence (called 'Events'). Alarm ON/OFF Status is provided by reading 16-bit holding registers (Modbus Function 03) with a single bit designated per input. A 48 input system would indicate the status of all alarms using three 16-bit holding registers. If the 61850 feature was enabled in the SER^{NET} this would require an additional three 16-bit holding registers for the IEC61850 points . The Modbus implementation also allows the transmitting or receiving of the Acknowledge function. Upon receiving an Acknowledge input, it will perform the same functionality as the Acknowledge button on the WEB Browser, such as acknowledging alarms on various screens, changing the LED indicators on the SER^{NET} unit from flashing to steady and de-activating a horn output if used. The Acknowledge operation performed by the web browser or external acknowledge pushbutton input can be transmitted through the Modbus protocol.

Event Data is provided by reading six 16-bit holding registers (Modbus Function 03) that contain the time, date, input number and alarm status for each event. An event could be an input going into alarm or returning to normal. Event data is provided in blocks of ten events for a total of sixty 16-bit holding registers. If there are no new events since the last Modbus poll, it will return all FF's. If there are more than 10 events in the buffer, then it will continue to submit 10 events every poll until there are no new events.

Modbus Operation as a Stand-Alone or Slave Unit

The Modbus data from a Stand-Alone or Slave SER^{NET} unit will provide the ON/OFF Status and timestamp of each alarm in that unit for the 16, 32 or 48 channels depending on system size.

Modbus Master: In this configuration, the Modbus Port is configured as a Master, with connection to up to 3 Modbus Slave devices. For 'Alarm' ON/OFF status, you can select all or specific inputs by checking the input number box. The Modbus Start address can be configured based on the application. The ending address will automatically be presented based on the number of inputs selected. Example: If all 48 alarms are selected, it will require three 16 bit registers, 32 alarms will require 2 registers, 16 alarms will require 1 register, etc. If the 61850 feature was enabled in the SER^{NET} this would require double the 16-bit holding registers for the IEC61850 points. If you use the receiving or transmitting of the Acknowledge pushbutton controls, it will add an extra register to the list.
For Event data, you will select a Modbus Start address and the ending address will automatically increment by 60 (for 10 events).

Modbus Slave: In this configuration, the Modbus Port is configured as a Slave, with connection to a Modbus Master device. With Modbus TCP/IP, multiple Modbus Masters can connect to our SER^{NET} Slave. The Modbus Start address can be configured based on the application. The ending address will automatically be presented based on the number of inputs selected. Example: If the SER^{NET} unit has 48 alarms, it will require three 16 bit registers, 32 alarms will require 2 registers, 16 alarms will require 1 register, etc. If the 61850 feature was enabled in the SER^{NET} this would require double the 16-bit holding registers for the IEC61850 points. If you use the receiving or transmitting of the Acknowledge pushbutton controls, it will add an extra register to the list.
For Event data, you will select a Modbus Start address and the ending address will automatically increment by 60 (for 10 events).

Modbus Operation with MWEB SER^{NET} Systems

When the system is configured with the MWEB option, the Master SER^{NET} will provide the ON/OFF Status and timestamp of each alarm in the complete system, inclusive of all Slave SER^{NET} units connected to the Master. For example, if the SER^{NET} system had one Master and 3 slave units with 48 inputs each, the total quantity of inputs represented by the Master SER^{NET} Modbus would be 192. With the Modbus & DNP protocols, all point numbers throughout the network are contiguous and unique. Note that all remote devices must be connected with the Combined SER (MWEB) configuration screen before the virtual point numbers are assigned. For example, with a 48-point master and two 48-point remote devices; points will be numbered 1–48 (Master), 49–96 (remote 1) and 97–144 (remote 2). This virtual point numbering scheme is automatically set up at the time MWEB is enabled and remains intact until MWEB is disabled

Modbus Master: In this configuration, the Modbus Port is configured as a Master, with connection to a single Modbus Slave device. The Modbus Start address can be configured based on the application. The ending address will automatically be presented based on the number of inputs selected. Example: If the SER^{NET} system had 160 alarms, it will require ten 16 bit registers. For Event data, you will select a Modbus Start address and the ending address will automatically increment by 60 (for 10 events). Event data will be provided for all inputs in the system. Each event will include the input number.

Modbus Slave: In this configuration, the Modbus Port is configured as a Slave, with connection to a Modbus Master device. With Modbus TCP/IP, multiple Modbus Masters can connect to our SER^{NET} Slave. The Modbus Start address can be configured based on the application. The ending address will automatically be presented based on the number of inputs in the system. Example: If the SER^{NET} system has 480 alarms, it will require thirty 16 bit registers.

For Event data, you will select a Modbus Start address and the ending address will automatically increment by 60 (for 10 events). Event data will be provided for all inputs in the system. Each event will include the input number.

Modbus Alarm Data Mapping - Input Status (ON/OFF)

The system can present raw field input point data. Every poll of our device will show the current status of each input with a 1 representing an input in alarm and a 0 representing an input in the normal mode. This is not a representation of the Field Contact Input status which can be set for N.O. or N.C. operation, but the true state of each alarm input.(Alarm or Normal)

The Modbus implementation also allows the transmitting or receiving of the Acknowledge function. A Logic 1 indicates the Acknowledge function is activated and a Logic 0 indicates no pushbutton.

Data is again presented in a 16-bit register format.

The Modbus Map for a SER^{NET} Device is shown below.

Modbus Address	Bit 15	……	……	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
40001	AP 16			AP 07	AP 06	AP 05	AP 04	AP 03	AP 02	AP 01
40002	AP 32									AP 17
40003	AP 48									AP 33
40004	IP 64			IP 55	IP54	IP 53	IP52	IP 51	IP 50	IP 49
40005	IP 80									AP 65
40006	IP 96									AP 81
40007							ACK rx		ACK tx	

AP = Digital Alarm Point #

IP = IEC61850 Alarm Point #

ACK = Acknowledge Function (rx = receive, tx = transmit)

Note: 48 Point unit showed above with a Modbus starting address of 40001 . If the unit is provided with 16 Alarm Inputs, one 16 bit register is used. If the unit is provided with 32 Alarm Inputs, two 16 bit registers are used. If the Modbus data is coming from a SER^{NET} MWEB Master, it will provide the corresponding number of registers. For example, a 480 input system would provide thirty 16-bit registers. (40001 thru 40030)

Modbus Event Data Mapping (Status + Time Stamp)

Event data may be read in blocks of 10 events at a time. These appear in a block of 60 registers (6 per event). Once ten events are read then the registers are reloaded with any subsequent ones from the event buffer until all events are retrieved. If no event has occurred, then all sixty registers are filled with FF HEX.

The event data format is as shown below:

16-bit Word	MSB (bit positions 8 - 15)	LSB (bit positions 0 - 7)
1	Year	Month
2	Day	Hour
3	Minute	Second
4	Millisecond	
5	Input Point Number	
6	IRIG-B Status [0 = off, 1 = on]	Input Status [0= Alarm, 1=Normal]

An example of the register format for 10 events is shown below.

Modbus Address	Event #	Modbus Data	
		MSB (bit positions 8 - 15)	LSB (bit positions 0 - 7)
41001	1	Year [0-99]	Month [1-12]
41002		Day [1-31]	Hour [1-24]
41003		Minute [1-60]	Second [1-60]
41004		Millisecond [0-999]	
41005		Input Point Number [1-1200]	
41006		IRIG-B Status [0 = off, 1 = on]	Input Status [0= Alarm, 1=Normal]
41007	2	Year [0-99]	Month [1-12]
41008		Day [1-31]	Hour [1-24]
41009		Minute [1-60]	Second [1-60]
41010		Millisecond [0-999]	
41011		Input Point Number [1-1200]	
41012		IRIG-B Status [0 = off, 1 = on]	Input Status [0= Alarm, 1=Normal]
41055	10	Year [0-99]	Month [1-12]
41056		Day [1-31]	Hour [1-24]
41057		Minute [1-60]	Second [1-60]
41058		Millisecond [0-999]	
41059		Input Point Number [1-1200]	
41060		IRIG-B Status [0 = off, 1 = on]	Input Status [0= Alarm, 1=Normal]

Modbus Addresses

Conventional addresses are included in the configuration. The input and output functions here are the most common and refer to a system in slave configuration.

Conventional Start address	Data	Input Functions	Output Functions
00000	Output Coils	05,15	01
10000	Discrete Inputs		02
30000	Input Registers		04
40000	Holding (output) Registers	06,16	03
60000	Extended Memory		

Default Values

Designation	Options	Default	Comments
Modbus Address	0-255	01	
Receive Start Address	40001-49999	40001	Register address entry.
Transmit Start Address	40001-49999	40001	
Modbus Mode	Master/Slave	Slave	Is this system Modbus Master?
Data type	AN3135 Style AN3135/Point/State	Point	An3135 mimic, point or alarm state data.
Baud rate	2400/4800/ 9600/19200	9600	
Parity	Odd/Even/none	None	Parity type
Transmit controls	Yes/No		Send alarm control (ACK, RST) data
Data direction	Input/output	Output	1 bit per point to designate Tx/Rx data
Modbus format	ASCII/RTU	RTU	

Default Baud Rate – change to 19200 in table above

Appendix B

DNP Data Formats

The DNP Communication option is used to transmit point status (Binary Inputs) and time stamped events (Binary Input Change with Time). The DNP Communications work in a slave mode and operate over RS-232/485 or Ethernet. The DNP implementation is outlined in the Device Profile Document.

Device Profile Document

<table>
<tr><td colspan="2">DNP V3.0
DEVICE PROFILE DOCUMENT</td></tr>
<tr><td colspan="2">Vendor Name: AMETEK Power Instruments</td></tr>
<tr><td colspan="2">Device Name: SER^{NET}, using the Triangle MicroWorks, Inc. DNP3 Multi-Port Slave Source Code Library</td></tr>
<tr><td>Highest DNP Level Supported:
For Requests: Level 2
For Responses: Level 2</td><td>Device Function:
Slave</td></tr>
<tr><td colspan="2">Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table):
For static (non-change-event) object requests, request qualifier codes 00 and 01 (start-stop), and 17 and 28 (index) are supported in addition to request qualifier code 06 (no range – or all points). Static object requests received with qualifiers 00, 01 or 06, will be responded to with qualifiers 00 or 01. Static object requests received with qualifiers 17 or 28 will be responded to with qualifiers 17 or 28. For change-event object requests, qualifier codes 06 (no range) and 07 and 08 (limited quantity) are supported. Qualifiers 17 or 28 are always returned.</td></tr>
<tr><td>Maximum Data Link Frame Size (octets):
Transmitted: 292
Received 292</td><td>Maximum Application Fragment Size (octets):
Transmitted: Configurable up to 2048
Received 2048</td></tr>
<tr><td>Maximum Data Link Re-tries:
Configurable from 0 to 255</td><td>Maximum Application Layer Re-tries:
None</td></tr>
<tr><td colspan="2">Requires Data Link Layer Confirmation:
Configurable as: Never, Only for multi-frame messages, or Always</td></tr>
<tr><td colspan="2">Requires Application Layer Confirmation:
When sending multi-fragment responses (Slave devices only)
Sometimes</td></tr>
<tr><td colspan="2">Timeouts while waiting for:
Data Link Confirm: Configurable.
Complete Appl. Fragment: None
Application Confirm: Configurable.
Complete Appl. Response: None</td></tr>
</table>

Sends/Executes Control Operations: WRITE Binary Outputs **Never** SELECT/OPERATE **Always** DIRECT OPERATE **Always** DIRECT OPERATE – NO ACK **Always** Count > 1 **Never** Pulse On **Always** Pulse Off **Always** Latch On **Always** Latch Off **Always** Queue **Never** Clear Queue **Never**	
Reports Binary Input Change Events when no specific variation requested: **Never**	Reports time-tagged Binary Input Change Events when no specific variation requested: **Never**
Sends Unsolicited Responses: **Never**	Sends Static Data in Unsolicited Responses: **Never** No other options are permitted.
Default Counter Object/Variation: Default Object 1 Default Variation: 1	Counters Roll Over at: **No Counters Reported**
Yes	

Implementation Table

OBJECT			**REQUEST**	**RESPONSE**	
Object Number	**Variation Number**	**Description**	**Function Codes (decimal)**	**Function Codes (decimal)**	**Qualifier Codes (hex)**
1	1	Binary Input	1 (read)	129 (response)	00, 01 (start-stop) 17,28 (Index)
2	2	Binary Input Change with Time	1 (read)	129 (response)	00, 01 (start-stop) 17,28 (Index)
10	2	Binary Output Status	1 (read)	129 (response)	00, 01 (start-stop) 17,28 (Index)
12	1	Control Relay Output Block	3,4,5,6	129 (response)	00, 01
50	1	Time and Date	1 (read)	129 (response)	07
60	1	Class 0 Data	1 (read)	129 (response)	
60	2	Class 1 Data	1 (read)	129 (response)	
60	3	Class 2 Data	1 (read)	129 (response)	
60	4	Class 3 Data	1 (read)	129 (response)	

SER^{NET} Data Map

Binary Inputs

Each Object 1, Variation 1 request will provide the status (on/off) of all SER^{NET} inputs as shown below. This is not the status of the alarm contact (open/closed), but whether an input is in alarm or has returned to normal. Alarms are reflected as a '1' and Normal inputs are '0'.

Index #	DNP Object		Description
	Object Number	Variation Number	
00	01	01	Point 1 Digital Contact Alarm
01	01	01	Point 2 Digital Contact Alarm
02	01	01	Point 3 Digital Contact Alarm
03	01	01	Point 4 Digital Contact Alarm
04	01	01	Point 5 Digital Contact Alarm
05	01	01	Point 6 Digital Contact Alarm
06	01	01	Point 7 Digital Contact Alarm
07	01	01	Point 8 Digital Contact Alarm
08	01	01	Point 9 Digital Contact Alarm
09	01	01	Point 10 Digital Contact Alarm
10	01	01	Point 11 Digital Contact Alarm
1196	01	01	Point 1197 Digital Contact Alarm
1197	01	01	Point 1198 Digital Contact Alarm
1198	01	01	Point 1199 Digital Contact Alarm
1199	01	01	Point 1200 Digital Contact Alarm

Note: The number of Index's (point #) is based on the system size.
For example: A stand-alone 48 channel unit will include Index # 00-47.
A distributed MWEB system with (1) Master 48 channel unit and (24) Slave 48 channel units will include index # 00-1199 as shown above.

Binary Input Change with Time

The time stamped alarms are presented as Binary Input Changes with Time as shown below: An event includes any change of status (inputs going to the alarm state or inputs returning to normal).

DNP Object		Description
Object Number	Variation Number	
02	02	Digital Contact Alarm w/time of event

These events will be reported as they occur and will include the input number and time stamp.

Binary Output Status

This DNP object will provide the status of the Acknowledge Pushbutton, when operated by the WEB Browser, external Acknowledge Pushbutton Input or via communications.

Index #	DNP Object		Description
	Object Number	Variation	
01	10	2	Acknowledge Pushbutton

The value of Index 01 will be a '1' when there has been an Acknowledge performed within the last 5 seconds. A value of '0' will reflect no pushbutton operation.

Control Relay Output Block

This DNP object is used to transmit the Acknowledge function to the SER^{NET}.

Index #	DNP Object		Description
	Object Number	Variation	
01	12	1	Acknowledge Pushbutton
Mode: Direct 16Bit Index Control Code: LON, LOFF			
For proper operation: Two commands should be sent, a LON control code followed by the LOFF code. The Acknowledge is executed upon the LON receipt. If a LOFF is not received with-in 5 seconds, it is automatically reset, so that subsequent LON controls would be accepted.			

Time and Date

This DNP Object is used to set the SER^{NET} clock with the time and date. It uses the Absolute Time which is recorded as milliseconds since midnight, January 1st, 1970, at zero hours, zero minutes, zero seconds, and milliseconds.

DNP Object		Description
Object Number	Variation Number	
50	01	Time and Date

Appendix C Bacnet Data Formats

Appendix D SNMP

Appendix E Replacement/Spare Parts/Accessories:

Ethernet Switch - 5 Port, Industrial Hardened

Ethernet Switch - 8 Port, Industrial Hardened

Remote Access Switch - 5 Ethernet Ports, 1 Internal 56K modem, Industrial Hardened

External 48Vdc to 24vDC Power Supply

External 125Vdc Output Field Contact Voltage Supply (AC/DC Input)

GPS Clock, IRIG-B Output

GPS Clock, NTP Output

Appendix F Browser Compatibility

If using Internet Explorer you must disable the caching of web pages.

To disable caching with Microsoft Internet Explorer V7

1 Choose **Internet Options** from the **Tools** menu. The Internet Options window opens.

2 On the **General** tab, in the **Browsing History** group, Click **Settings**. The Settings window opens.

3 Make sure that the “Check for newer versions of stored pages” option is set to Every time I visit the web page.

4 Click **OK** to close the Settings window.

5 Click **OK** to close the Internet Options window.

To disable caching with Microsoft Internet Explorer (v5 only)

1 Choose **Internet Options** from the **Tools** menu. The Internet Options window opens.

2 Click **Settings** in the **Temporary Internet files** group. The Settings window opens.

3 Make sure that the Check for newer versions of stored pages option is set to Every visit to the page.

4 Click **OK** to close the Settings window.

5 Click **OK** to close the Internet Options window.

To disable caching with Microsoft Internet Explorer 4.01 to 5

1 Choose **Internet Options** from the **View** menu. The Internet Options window opens.

2 In the **General** tab’s **Temporary Internet Files** group, click the **Settings** button. The Settings window opens.

3 Make sure that the Check for newer versions of stored pages option is set to Every visit to the page.

4 Click **OK** to close the Settings window

5 Click **OK** to close the Internet Options window.

To disable caching with Microsoft Internet Explorer on Mac OS

1 Choose **Preferences** from the **Edit** menu. The Internet Explorer Preferences window opens with a list of preference categories on the left side of the window.

2 Locate and click **Advanced** (listed under **Web Browser**). The advanced options for the browser are displayed in the right side of the window.

3 In the **Cache** group, choose **Always** for the **Update pages** option.

4 Click **OK** to save your options and close the window.

To disable caching with Netscape Navigator

1 Choose **Preferences** from the **Edit** menu. The Preferences window opens.

2 In the **Category** group (left frame), click the **plus sign (+)** next to the **Advanced** category.

3 Under **Advanced**, select the **Cache** option. The right side of the Preferences window changes to the Cache options.

4 At the bottom of the Cache group of options, be sure that the **Document in cache is compared to document on network** option is set to **Every time**.

5 Click **OK** to close the Preferences window.

The SER^{NET} IP address must be in the trusted zone. Or, in IE, you will see a yellow bar with a script warning when you try to download a .csv file, follow these steps to configure your browser.

To add your SER^{NET} to the trusted zone:

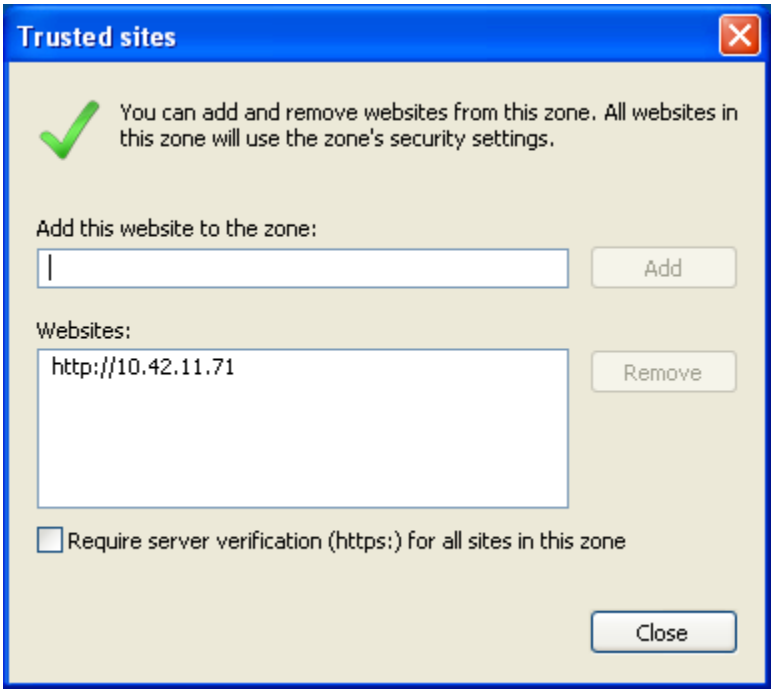
1. From within Internet Explorer, click “Tools”, in the drop-down menu, click “Internet Options”.

2. In the “Internet Options” dialog box, select the “Security” tab.

3. From Zones, select “Trusted sites” (large check mark).

4. Below Zones and next to “Trusted sites”, click the “Sites” button.

5. You will be prompted with the following:



Enter your unit's IP address in the top field and click the "Add" button which will add the IP address to the trusted zone.

6. Click Close, then OK.

Appendix G Notes on saving the event file as .csv

Opening the .csv file with Excel corrupts the time column.

When saving the event file as a .csv and then opening this file with Excel, the data in the time column gets corrupted. The reason is that Excel automatically formats this column as a type "general" and therefore tries to interpret the time as a number.

The work around is to save the file as a .txt, and then when opening this file with Excel tell Excel to format the time column as text.

Download .csv button prompts a yellow script bar blocking the yes/no question box.

The SER^{NET} IP address must be in the trusted zone. Or, in IE, you will see a yellow bar with a script warning when you try to download a .csv file, follow these steps to configure your browser.

To add your SER^{NET} to the trusted zone:

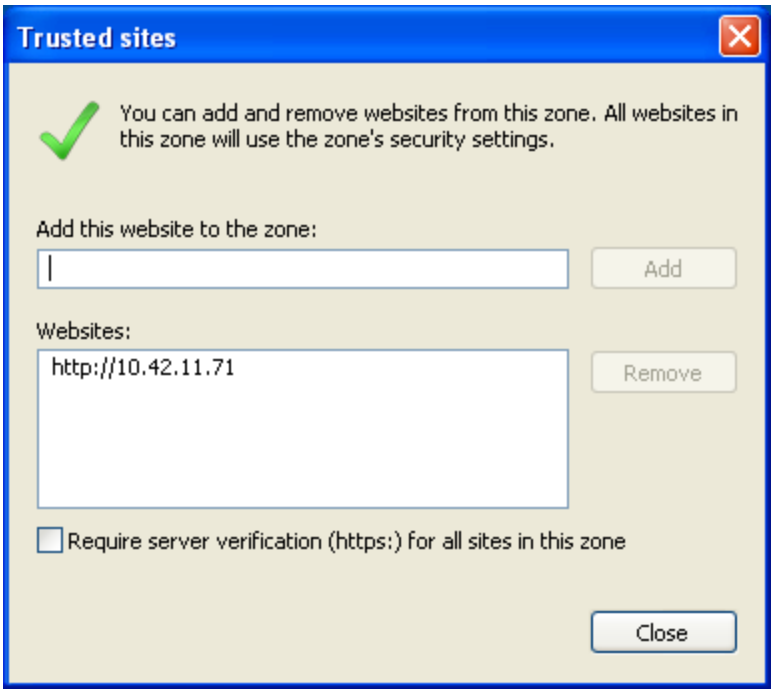
1. From within Internet Explorer, click "Tools", in the drop-down menu, click "Internet Options".

2. In the "Internet Options" dialog box, select the "Security" tab.

3. From Zones, select "Trusted sites" (large check mark).

4. Below Zones and next to "Trusted sites", click the "Sites" button.

5. You will be prompted with the following dialog box:



Enter your unit's IP address in the top field and click the "Add" button which will add the IP address to the trusted zone under "Websites".

6. Click Close, then OK.

Formatting the Excel .csv file for milliseconds

Excel does not have a standard number format for milliseconds. It can be added using the custom formatting.

1. Select the top timestamp in your spreadsheet.
2. Right click the cell and select Format Cells
3. Under Number, select Custom
4. The format should present hh:mm:ss.0
5. Add two extra 0's so it looks like this: hh:mm:ss.000
6. Copy this format to all cells in this column

Appendix H Default Settings

Default Settings of Main Board
Alarm Inputs:

Input Enabled: All set to enabled

Filter Mode: All set to Filter time

Filter Time: All set to 0

Auto DFS: All set to 0

Alarm Legends: Are Never Changed from user settings. From factory they are set to “Input X is in Alarm”

Alarm Legends: Are Never Changed from user settings. From factory they are set to “Input X has returned to Normal”

Alarm Output 1: Coil State is Energized; Relay Function is Watchdog

Alarm Output 2: Coil State is De-energized; Relay Function is Alarm

Appendix I Diagnostic Events

The following diagnostic events could be reported in the Event Log.

M = Master

S = Slave

Unit	Diagnostic Events (Descriptor 'D')	Description
Configuration Related Events		
M/S	Configuration Changed via WEB	Alarm Inputs/Outputs configuration Change
M/S	Configuration Changed via File Restore	Alarm Inputs/Outputs configuration Change by importing a configuration file via the web page Restore feature
M/S	Enabled Alarm Input via WEB Page	Alarm manually enabled via configuration
M/S	Disabled Alarm Input via WEB Page	Alarm manually disabled via configuration
System Operational Events		
M/S	Alarm Acknowledged	Alarm Acknowledged via the browser at the same unit
M	Remote Alarm Acknowledged	Alarm Acknowledged at the Master browser for a Slave unit
S	Alarm Acknowledged at Remote Master	Alarm Acknowledged at the Master browser for a Slave unit
M/S	Restored to Scan	Auto Delete from scan de-activated for a repetitive alarm
M/S	Off Scan	Auto Delete from Scan activated for a repetitive alarm
M/S	SER Buffer Overflow	The number of alarms received exceeded the capability of the unit 80 events/sec x 35 inputs for several minutes
M/S	Lost a maximum of X events.	This event may occur in conjunction with an "SER Buffer Overflow" event. An attempt is made to recover the lost event(s).
Power Related Events		
M/S	Main Board Power On	Unit powered up or configuration just performed which took the system off line
M/S	Power Loss / Reboot	Loss of power or unit powered down automatically during a firmware upgrade
M/S	Power Restored / Reboot Complete	Power restored or unit powered up automatically during a firmware upgrade
Combined SER (MWEB) Events		
M	Connected to Remote Device at *Station ID*	Master unit connected to Slave unit (occurs during initial set-up)
M	Disconnected from Remote Device at *Station ID*	Master unit manually disconnected from Slave unit
M	Slave at Station ID no longer responding	Master unit no longer communicating to the Slave
S	Master Combined SER at Station ID Disconnected	Slave unit identifying that it is no longer connected to a Master
S	Master Combined SER at Station ID Connected	Slave unit identifying that it has been connected to a Master
M	Alarm Out of Sync Forced ON	When a Master Reconnects to a Slave, any existing Slave alarms are treated at the Master as new alarms
M	Alarm Out of Sync Forced OFF	When a Master disconnects from a Slave, any existing Slave alarms at the Master are automatically returned to normal

Unit	Diagnostic Events (Descriptor 'D')	Description
Serial and Ethernet Communications		
M/S	Modbus RTU Master Response Error: Invalid response from Slave (Slave Address #)	Serial Modbus Master did not receive a response from the Slave unit
M/S	Modbus RTU Master Response Error (Exception from Slave (Slave Address #)	Serial Modbus Master received an Exception from this slave
M/S	Modbus RTU Master Response Error (Address Error from Slave (Slave Address #))	Serial Modbus Master received an invalid address request from this slave
M/S	Modbus RTU Master Response Error (No response from Slave (Slave Address #))	Serial Modbus Master received no response from this slave
M/S	Ethernet Modbus Master Failed to connect to (Slave IP Address)	Modbus TCP/IP Master did not receive a response from the Slave unit
M/S	Ethernet Modbus Master successfully connected to (Slave IP Address)	Modbus TCP/IP Master connect to slave after failure.
M/S	Ethernet Modbus Master Response Error (Exception from Slave (Slave Address #))	Modbus TCP/IP Master received an Exception from this slave
M/S	Ethernet Modbus Master Response Error (Address Error from Slave (Slave Address #))	Modbus TCP/IP Master received an invalid address request from this slave
M/S	Ethernet Modbus Master Response Error (No response from Slave (Slave Address #))	Modbus TCP/IP Master received no response from this slave
M/S	Ethernet Modbus Master Response Error (MBAP transaction id error from slave (Slave Address #))	Modbus TCP/IP Master found a transaction problem with the MBAP (ethernet message header)
M/S	Ethernet Modbus Master Response Error (MBAP protocol id error from slave (Slave Address #))	Modbus TCP/IP Master found a protocol error in the MBAP (ethernet message header)
M/S	Serial Port Timed out	When configured for Serial Comms Ascii Protocol this indicates a failure to write to the serial port after waiting for 1 minute.
M/S	Failed to initialize serial port	Indicates a hardware failure of the serial port.
Firmware Upgrade Events		
M/S	Error opening file jffs/update/sernetmainboard.S19	Indicates a failure during firmware upgrade.
M/S	FAILED to update firmware on main board	Indicates a failure during firmware upgrade reported by the Web Board.
M/S	Firmware Update Succeeded	This is a message to indicate that the firmware update was completed OK.
M/S	Firmware Update Failed	If the firmware update to the Main Board has failed you will see this event.

Unit	Diagnostic Events (Descriptor 'D')	Description
Internal Communication Events		
M/S	Cold Start with Default Settings	This should only occur if the main board is jumpered to reinitialize the Alarm Input/Output configuration
M/S	Received invalid Event code(X) for input number(Y)	Main Board firmware is out of date with Web board firmware; (Should Not occur)
M/S	Communications Failure with Main Board	This event may occur immediately after a firmware upgrade. It is usually pared with the event "Communications Restored with main Board". If you do not see the Restored event then a hardware failure has occurred.
M/S	Communications Restored with Main Board	When an internal communications failure occurred but has been corrected you will see this events. Should only occur after a firmware upgrade.

Unit	Time Sync Events (Descriptor 'T')	Description
M/S	Hourly Time Update	Time updated on the hour successfully between the Main Board and WEB Board
M/S	Obtained IRIG-B Synchronization	IRIG-B Time Sync signal detected
M/S	Lost IRIG-B Synchronization	The IRIG-B Time Sync signal was lost
M/S	Obtained IRIG-B Synchronization	IRIG-B Time Sync signal detected
M/S	Lost IRIG-B Synchronization	The IRIG-B Time Sync signal was lost
S	Obtained Serial Synchronization	Slave unit has synchronized it's time to the master via the RS485 time sync
S	Lost Serial Synchronization	Slave unit has lost it's synchronization to the master via the RS485 time sync

Appendix J Legend Format for CSV Import

The following formatting instructions for the csv import file must be followed:

1. The first value must be the point number you wish to update 1->48; this must be followed by a comma character.
   For MWEB (Combined SER) systems, the input numbers in your file should match the input channel assignments, ex. Master SER has inputs 1-48, slave 1 has inputs 49-96, etc
2. The second field is the text string you want loaded for Alarm Legend. If there is a separate legend for the normal state, enter a comma after the Alarm legend. The max length for the Alarm Legend is 32 characters; therefore; only the first 32 characters will be stored.
3. The 3rd field is the text string you want loaded for Normal Legend; this string MUST NOT contain any commas. The max length for the Normal Legend is 32 characters; therefore; only the first 32 characters will be stored.

An example of a valid entry is: **1, Input 1 is in Alarm, Input 1 has returned to Normal**

Additional Notes:

- Lines beginning with a # character indicate a comment line; these are allowed as they are not processed
- Only include lines for inputs you wish to change either the Alarm Legend or Normal Legend. If you only wish to update the Alarm Legend; you may skip entering the 3rd field as defined above in 3. For example:
  1, Fire Alarm
  This a valid entry and will modify only the Alarm Legend for input 1.

If you only wish to update the Normal Legend; you must still enter it as the 3rd field as defined above in 3; but you can skip modification of the Alarm Legend by not entering any characters between the commas. For example:
1, , Fire Alarm has returned to Normal
This a valid entry and will modify only the Normal Legend for input 1.
Note: if you put a space between the 2 commas above it will be interpreted as entering a single space for the Alarm Legend and this would clear out any previous entry.

Appendix K IEC 61850 Protocol

The IEC 61850 Protocol Option can be used in several variations:

- It can subscribe to an IEC 61850 enabled device and retrieve the alarm status using GOOSE messaging. It has the option to use the time stamp from the IEC 61850 device or use the time stamp when the alarm is received by the SER^{NET}.
- It can be used for retransmitting the SER^{NET} digital input alarm status to other IEC 61850 devices using GOOSE messaging.
- It can be used retransmit the SER^{NET} alarm outputs to other IEC 61850 devices using GOOSE messaging.
- It can be used as an IEC 61850 Server, publishing the status of the SER^{NET} digital inputs and alarm outputs using Buffered and Un-Buffered reports.

The IEC 61850 alarms received by the SER^{NET} can be displayed on the WEB Browser Graphic Screen. The IEC 61850 alarms will be merged with the 'digital' contact inputs for one common WEB Browser display using the Active Alarm page and Event Log. In addition the alarms can be used to trigger an email, or can be re-transmitted using the Modbus and DNP Protocols. This allows a bridge between IEC 61850 alarms and legacy equipment that use the Modbus / DNP Protocols.

IEC 61850 Configuration

The IEC 61850 Configuration process starts with our AMETEK 61850 Configuration Software which maps the IEC 61850 devices to and from the SER^{NET}. Each SER^{NET} model (16, 32, 48 inputs) has it's own 61850 ICD file which is included in the software. This ICD file describes all the features of the SER^{NET} Sequence of Events Recorder to enable interconnection to other IEC 61850 devices. The ICD files of other 61850 enabled devices that will connect to the SER^{NET} need to imported into the configuration software along with the SER^{NET} ICD file. The inputs and outputs of these devices are mapped together using the software and the end result is the creation of a CID file which is sent to the SER^{NET}. This provides the necessary connections between devices once installed.
This process is further detailed in the 61850 Configuration Software Manual.

GOOSE Messaging

The SER^{NET} supports GOOSE messaging from another IED to receive changes of alarm status or to transmit GOOSE messages derived from one of the SER^{NET} hardwired binary inputs.

- GOOSE Receive – The software shall allow the connection of multiple IED's and map specific data items (alarms) to the SER^{NET} inputs
- GOOSE Transmit – The software shall allow you to select any of the SER^{NET} hardwired digital inputs and configure them for use in a 61850 network.

Device Information

The SER^{NET} will support the following logical nodes:

Logical Node	Name	Description
Physical Device	LPHD	Power-up detected (PwrUp), Power-down detected (Pwr-Dn), Power Supply Alarm (PwrSupAlm)
Generic I/O	GGIO	Status: Integer status input (IntIn), General single alarm (Alm), General indication - binary input (Ind)

Physical Device (LPHD)

The Physical Device (LPHD) will consist of the following items.

Attribute Name	Description
LNName	LPHD
PHYNam	Device Nameplate
PHYHealth	Health

Generic Process I/O (GGIO)

The Generic Process I/O will consist of the following items.

Attribute Name	Attribute Type	Description
LNName		GGIOSer
Common Logical Node Information		
EEHealth		Health
EEName		Nameplate
Status Information		
Ind1	SPS	SERNET Alarm 1 (Binary Input)
Ind2	SPS	SERNET Alarm 2 (Binary Input)
Ind3	SPS	SERNET Alarm 3 (Binary Input)
Ind4	SPS	SERNET Alarm 4 (Binary Input)
Ind5	SPS	SERNET Alarm 5 (Binary Input)
|		|
Ind47	SPS	SERNET Alarm 47 (Binary Input)
Ind48	SPS	SERNET Alarm 48 (Binary Input)
Alm1	SPS	SERNET Alarm 1 (61850 Input)
Alm2	SPS	SERNET Alarm 2 (61850 Input)
Alm3	SPS	SERNET Alarm 3 (61850 Input)
Alm4	SPS	SERNET Alarm 4 (61850 Input)
Alm5	SPS	SERNET Alarm 5 (61850 Input)
|		|
Alm47	SPS	SERNET Alarm 47 (61850 Input)
Alm48	SPS	SERNET Alarm 48 (61850 Input)

PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (PICS)

1.1 Introduction

This specification is the Protocol Implementation Conformance Statement (PICS) and presents the ACSI conformance statements as defined in Annex A of Part 7-2 of the IEC 61850 standard specifications.

1.2 ACSI basic conformance statement

The basic conformance statement shall be as defined in Table A.1.

TABLE A.1 –Basic Conformance Statement

		Server/ Publisher/ Subscriber	***Remarks***
Client -Server Roles			
B11	**Server** Side (of TWO-PARTY-APPLICATION-ASSOCIATION)	YES	Capability of an IED to expose its data to external IEC 61850 Clients
B12	**Client** Side (of TWO-PARTY-APPLICATION-ASSOCIATION)	NO	Capability of a Client to access data from external IEDs (IEC 61850 Servers)
SCSMs supported			
B21	**SCSM**:IEC 61850-8-1 used	YES	Station Bus protocol support of an IED via IEC 61850 Server (MMS) and GOOSE (Multi cast Ethernet Messaging)
B22	**SCSM**:IEC 61850-9-1 used	NO	Process Bus Protocol Support of an IED via Sampled Value (Uni cast Ethernet messaging)
B23	**SCSM**:IEC 61850-9-2 used	NO	Process Bus Protocol Support of an IED via Sampled Value (Multi cast Ethernet Messaging)
B24	**SCSM**: other	NO	
Generic Substation event Model(GSE)			
B31	**Publisher** side	YES	Publish System Events via GOOSE (Multi cast Ethernet Messaging)
B32	**Subscriber** Side	YES	Receive System Events via GOOSE (Multi cast Ethernet Messaging)
Transmission of Sampled value model (SVC)			

B41	**Publisher** side	NO	Publish Sampled Value data via SMV (Multi cast Ethernet Messaging)
B42	**Subscriber** side	NO	Receive Sampled Value data via SMV (Multi cast Ethernet Messaging)

c1 - Shall be 'M' if support for **LOGICAL-DEVICE** model has been declared

O - Optional

M - Mandatory

1.3 ACSI models conformance statement

The ASCI models conformance statement shall be as defined in Table A.2

TABLE A.2 ACSI models Conformance Statement

		Server/ Publisher/ Subscriber	Remarks
If **Sever** side (B11) supported			
M1	**Logical Device**	YES	Categorization of Data within an IED like Protection, Control, Records, System etc. At least one is mandatory
M2	**Logical Node**	YES	Logical Functions available in an IED like LLN0, LPHD, GGIO etc. At least three are mandatory
M3	**Data**	YES	Data available in Logical Nodes like Indications and Alarms in GGIO
M4	**Data Set**	YES	Grouping of data to assign to Reports and GOOSE Publishers
M5	**Substitution**	NO	This service is Optional. This allows SERNET's internal logic or external IEC 61850 Client to substitute a GGIO Indication / Alarm value
M6	**Setting group control**	NO	This service is not valid in case of an Event recorder. This feature is to allow IEC 61850 Client to switch between different Protection schemes / settings available in IEDs
Reporting			
M7	**Buffered report control**	**YES**	Service allows IED to send Reports to IEC 61850 Client based on data / quality changes in Data set variable points
M7-1	Sequence – number	YES	A Report generated will have a Unique Identification Number which will be sent along with Report Data, if this option is enabled
M7-2	Report-time-stamp	YES	A Report generated will have a time stamp associated with it which will be sent along with Report Data, if this option is enabled
M7-3	Reason-for-inclusion	YES	A Report generated will have multiple variables and each of them were included because of certain trigger conditions. Reason-for-inclusion will be sent along with Report Data, if this option is enabled
M7-4	Data-set-name	YES	A Report generated will have a Dataset assigned to it whose name will be sent along with Report Data, if this option is enabled

M7-5	Data-reference	YES	A Report generated will have multiple variables. Their names will be sent along with Report Data, if this option is enabled
M7-6	Buffer-overflow	YES	A Report's buffer may overflow. Indication will be sent along with Report Data, if this option is enabled
M7-7	Entry id	YES	A Report generated will have a Unique Identification which will be sent along with Report Data, if this option is enabled
M7-8	Buf Tm	YES	Functionality to control the report generation frequency in case of a new event. Used to avoid very frequent report generation in case of related events
M7-9	IntgPd	YES	Functionality to control the report generation frequency in case of no events. Used to have periodic report generation in case of no events
M7-10	GI	YES	Functionality to control the report generation in case of no events. Used to have forced report generation in case of no events
M8	**Unbuffered report control**	**YES**	YES
M8-1	Sequence – number	YES	YES
M8-2	Report-time-stamp	YES	YES
M8-3	Reason-for-inclusion	YES	YES
M8-4	Data-set-name	YES	A Report generated will have a Dataset assigned to it whose name will be sent along with Report Data, if this option is enabled
M8-5	Data-reference	YES	A Report generated will have multiple variables. Their names will be sent along with Report Data, if this option is enabled
M8-6	Buf Tm	YES	Functionality to control the report generation frequency in case of a new event. Used to avoid very frequent report generation in case of related events
M8-7	IntgPd	YES	Functionality to control the report generation frequency in case of no events. Used to have periodic report generation in case of no events
M8-8	GI	YES	Functionality to control the report generation in case of no events. Used to have forced report generation in case of no events

	Logging	NO	Feature to store event log within the IED for later retrieval from Client. Acts like sequence of events storage within IED. Requires too much of RAM. Not popular in usage
M9	**Log control**	NO	Feature to store event log within the IED for later retrieval from Client. Acts like sequence of events storage within IED. Requires too much of RAM. Not popular in usage

M9-1	IntgPd	NO	Functionality to control the report generation frequency in case of no events. Used to have periodic report generation in case of no events
M10	*Log*	NO	Feature to store event log within the IED for later retrieval from Client. Acts like sequence of events storage within IED. Requires too much of RAM. Not popular in usage
M11	**Control**	NO	Service to operate DIGITAL outputs from IEC 61850 Client. Feature can be enabled as per the requirements
If **GSE** (B31/B32) is supported			
	GOOSE	YES	Functionality to support Sending and Receiving of GOOSE packets
M12-1	EntryID	NO	Not Supported
M12-2	DataReflnc	NO	Not Supported
M13	**GSSE**	NO	Depreciated as per new Edition of Standard. Not popular in Usage
If **SVC** (B41/B42) is supported			
M14	Multicast SVC	NO	To publish / subscribe Sampled Value Packets based on sampling Rate to Process bus
M15	Unicast SVC	NO	To publish / subscribe Sampled Value Packets based on sampling Rate to Process bus
M16	**Time**	YES	Support UTC with desired accuracy level
M17	**File Transfer**	NO	Transfer of files between IED and IEC 61850 Clients. This service is optional. Relevant in case of IEDs with File System Support

c2 – shall be 'M' if support for **LOGICAL-NODE** model has been declared

c3 – shall be 'M' if support for **DATA** model has been declared

c4 – shall be 'M' if support **DATA-SET**, Substitution, Report, Log Control, or Time model has been declared

c5 – shall be 'M' if support for Report , GSE, or SV model has been declared

M - Mandatory

1.4 ACSI service conformance statement

The ASCI service conformance statement shall be as defined in Table A.3

TABLE A.3 ACSI service Conformance Statement

	Services	**Server/ Publisher/ Subscriber**	***Remarks***
Server (Clause 6)			
S1	ServerDirectory	YES	Capability of IED (IEC 61850 Server) to provide its contents under Access Points to external IEC 61850 Clients
Application association (Clause 7)			
S2	Associate	YES	Capability of IED (IEC 61850 Server) to provide connections to Access Points from external IEC 61850 Clients
S3	Abort	YES	Capability of IED (IEC 61850 Server) to abort connections to Access Points from external IEC 61850 Clients
S4	Release	YES	Capability of IED (IEC 61850 Server) to close connections to Access Points from external IEC 61850 Clients
Logical device (Clause 8)			
S5	Logical Device Directory	YES	Capability of IED (IEC 61850 Server) to provide its contents under a Logical Device to external IEC 61850 Clients
Logical Node (Clause 9)			
S6	LogicalNodeDirectory	YES	Capability of IED (IEC 61850 Server) to provide its contents under a Logical Node to external IEC 61850 Clients
S7	GetAllDataValues	YES	Capability of IED (IEC 61850 Server) to provide values of all variables under a Logical Node to external IEC 61850 Clients through a single request

Data (Clause 10)			
S8	GetDataValues	YES	Capability of IED (IEC 61850 Server) to provide values of one or more variables to external IEC 61850 Clients through a single request
S9	SetDataValues	NO	Capability of IED (IEC 61850 Server) to allow write of values of one or more variables to external IEC 61850 Clients through a single request
S10	GetDataDirectory	YES	Capability of IED (IEC 61850 Server) to provide its contents under a Data Object to external IEC 61850 Clients
S11	GetDataDefinition	YES	Capability of IED (IEC 61850 Server) to provide type information (ASN1) of a variable to external IEC 61850 Clients
Data Set(Clause 11)			
S12	GetDataSetValues	YES	Capability of IED (IEC 61850 Server) to provide values of all variables under a Dataset to external IEC 61850 Clients through a single request
S13	SetDataSetValues	NO	Capability of IED (IEC 61850 Server) to allow writing values of all variables under a Dataset to external IEC 61850 Clients through a single request
S14	CreateDataSet	YES	Capability of IED (IEC 61850 Server) to allow creation of Datasets from external IEC 61850 Clients
S15	DeleteDataSet	YES	Capability of IED (IEC 61850 Server) to allow deletion of Datasets from external IEC 61850 Clients
S16	GetDataSetDirectory	YES	Capability of IED (IEC 61850 Server) to provide list of available Datasets from external IEC 61850 Clients
Substitution (Clause 12)			
S17	SetDataValues	NO	Capability of IED (IEC 61850 Server) to allow write of values of one or more variables to external IEC 61850 Clients through a single request
Setting group control (Clause 13)			
S18	SelectActive SG	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850

			Clients to Activate a Setting Group
S19	SelectEdit SG	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients to Select a Setting Group for Editing
S20	SetSGvalues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients to Edit values in a Setting Group
S21	ConfirmEditSGvalues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients to confirm a Setting Group Editing
S22	GetSGvalues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients to read values in active Setting Group
S23	GetSGCBvalues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients to read values in Setting Group Control Block
Reporting (Clause 14)			
Buffered report control block(BRCB)			
S24	Report	YES	Capability of IED (IEC 61850 Server) to send data set buffered reports to external IEC 61850 Clients based on Trigger Conditions and Option Fields
S24-1	Data-change(dchg)	YES	Capability of IED (IEC 61850 Server) to send data set reports to external IEC 61850 Clients based on Data change Trigger Condition
S24-2	qchg-change(qchg)	YES	Capability of IED (IEC 61850 Server) to send data set reports to external IEC 61850 Clients based on Quality change Trigger Condition
S24-3	Data-update(dupd)	NO	Capability of IED (IEC 61850 Server) to send data set reports to external IEC 61850 Clients based on Data update Trigger Condition
S25	GetBRCBValues	YES	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Buffered Report Control Block Values
S26	SetBRCBValues	YES	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients write Buffered Report Control Block Values
Unbuffered report control block(URCB)			
S27	Report	YES	Capability of IED (IEC 61850 Server) to send data set reports to external IEC 61850 Clients based on Trigger Conditions and Option Fields
S27-1	Data-change(dchg)	YES	Capability of IED (IEC 61850 Server) to send data set reports to external IEC 61850 Clients based on Data change Trigger Condition

S27-2	qchg-change(qchg)	YES	Capability of IED (IEC 61850 Server) to send data set reports to external IEC 61850 Clients based on Quality change Trigger Condition
S27-3	Data-update(dupd)	NO	Capability of IED (IEC 61850 Server) to send data set reports to external IEC 61850 Clients based on Data update Trigger Condition
S28	GetURCBValues	YES	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Unbuffered Report Control Block Values
S29	SetURCBValues	YES	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients write Unbuffered Report Control Block Values
c6 – shall declare support for at least one(BRCB or URCB)			
Logging(clause 14)			
Log Control block			
S30	GetLCBValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Log Control Block Values
S31	SetLCBValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients write Log Control Block Values
Log			
S32	QueryLogByTime	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Logs based on Time stamp
S33	QueryLogAfter	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Logs based on Unique Identification
S34	GetLogStatusValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Log Status
c7- shall declare support for at least one(query log by time or Query Log After)			
Generic Substation event model(GSE) (14.3.5.3.4)			
GOOSE – CONTROL - BLOCK			
S35	SendGOOSEMessage	YES	Capability of IED (IEC GOOSE) to send or receive GOOSE packets from / to network

S36	GetGOReference	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Goose Variable name
S37	GetGOOSEElementNumber	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Goose Variable Dataset Index
S38	GetGoCBValues	YES	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read GOOSE Control Block Values
S39	SetGoCBValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients write GOOSE Control Block Values
GSSE – CONTROL - BLOCK			
S40	SendGSSEMessage	NO	Capability of IED (IEC GOOSE) to send or receive GSSE packets from / to network
S41	GetGsReference	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Gsse Variable name
S42	GetGSSEElementNumber	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Gsse Variable Index
S43	GetGsCBValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read GSSE Control Block Values
S44	SetGsCBValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients write GSSE Control Block Values

c8- shall declare support for at least one(Send GOOSE Message or Send GSSE Message)

c9- shall declare support if TP association is available

Transmission of sampled value model(SVC) (Clause 16)

Multicast SVC

S45	SendMSVMessage	NO	Capability of IED (IEC SMV) to send or receive Sampled Value packets from / to network
S46	GetMSVCBValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Sampled Value Control Block Values
S47	SetMSVCBValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients write Sampled Value Control Block Values

Unicast SVC

S48	SendUSVMessage	NO	Capability of IED (IEC SMV) to send or receive Sampled Value packets from / to another IED
S49	GetUSVCBValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read Sampled Value Control Block Values
S50	SetUSVCBValues	NO	Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients write Sampled Value Control Block Values
C10- shall declare support for at least one(Send MSV Message or Send USV Message)			
control (17.5.1)			
S51	Select	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients Select a Control Object for Operation
S52	Select with value	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients Select a Control Object with value for Operation
S53	Cancel	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients Cancel a Selected Control Object
S54	Operate	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients Operate a Control Object
S55	Command-Termination	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to send extra status information to external IEC 61850 Clients regarding a Control Operation
S56	Time Activated-Operate	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients Operate a Control Object at a future Time

File Transfer (Clause 20)			
S57	GetFile	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read/retrieve a File
S58	SetFile	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients write/send a File
S59	DeleteFile	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients delete a File
S60	GetFileAttributeValues	NO	This is an optional Service. Capability of IED (IEC 61850 Server) to allow external IEC 61850 Clients read attributes of

				File(s) or directory
Time(5.5)				
T1	Time resolution of Internal clock	10 (1 msec)	Nearest negative power of 2 in seconds	Resolution of IED's internal Clock from where events are timestamped
T2	Time Accuracy of Internal clock	10 (1 msec)	T0	Accuracy at which events are timestamped
			T1	
			T2	
			T3	
			T4	
			T5	
T3	Supported Time Stamp resolution	10 (1 msec)	Nearest value of 2**-n in seconds according to 5.5.3.7.3.3	Resolution of TimeStamp variables of all events.

CONTACT LIST & WARRANTY

Telephone / Fax Number List

This errata sheet provides an easy-to-use reference for all major departments. Use these numbers for ordering equipment, application assistance, technical support, and scheduling field service

Please Note: Your instruction manual may contain other phone and fax numbers; this list will take precedence.

MAIN OFFICE

AMETEK Power Instruments – Rochester
255 North Union St., Rochester, NY 14605

DEPARTMENT/PRODUCT LINE	TELEPHONE	FAX
MAIN PHONE	585-263-7700	585-262-4777
FIELD SERVICE	800-374-4835	585-238-4945
REPAIRS/RETURNS	888-222-6282	585-238-4945
SALES SUPPORT	800-950-5503	585-454-7805

FAR EAST OFFICE

AMETEK Power Instruments
271 Bukit Timah Road, #03-09
Balmoral Plaza, Singapore 259708
Tel: 65-732-8675
Fax: 65-732-8676

UK OFFICE

AMETEK Power Instruments
Unit 20, Ridgeway
Donibristle Industrial Estate
Dunfermline, UK
Tel: 1383-825630
Fax: 1383-825715

Procedures for Factory Repair and Return

Obtain a Returned material Authorization (RMA) number by calling AMETEK Repair Sales and giving the following information:

Model and ***Serial Number*** of the equipment
Failure Symptom – **Be Specific**
Approximate date of installation
The site name and address of the failed equipment
Complete shipping information for the return of the equipment if other than the operating site
Name and telephone number of person to contact if questions arise.

Enclose the information with the equipment and pack in a commercially accepted shipping container with sufficient packing material to insure that no shipping damage will occur. Mark the outside of the container with the RMA number. Ship to the appropriate location: **Attention:** Repair Department

AMETEK Power Instruments
255 North Union Street
Rochester, New York 14605 USA
Tel: (888) 222-6282

Your emergency equipment will be tested, repaired and inspected at the factory. Factory turnaround is ten working days or less (excluding shipping time).

For emergency service or repair status information, please contact the AMETEK Repair Sales Engineer at (800) 374-4835.

Warranty

AMETEK warrants equipment of its own manufacture to be free from defects in material and workmanship, under normal conditions of use and service. AMETEK will replace any component found to be defective, upon its return, transportation charges prepaid, within one year of its original purchase. AMETEK will extend the same warranty protection on accessories that is extended to AMETEK by the original manufacturer. AMETEK assumes no responsibility, expressed or implied, beyond its obligation to replace any component involved. Such warranty is in lieu of all other warranties expressed or implied.