



SEL-3025 SCADA Shield Serial Cryptographic Transceiver

Secure SCADA Communication



The SEL-3025 SCADA Shield, an EIA-232 bump-in-the-wire serial cryptographic transceiver, protects meters, protective relays, Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), and computers from unauthorized access, control, monitoring, and malicious attack by authenticating and optionally encrypting all data along the communications path.

Major Features and Benefits

- **FIPS Compliant Design for Cryptographic Modules.** FIPS 140-2 Security Level 2 Validation.
- **Proven Cryptographic Serial Protocol.** Protect your data link with the Secure SCADA Communication Protocol (SSCP) by authenticating every data packet on your serial link. The SSCP can also provide strong encryption.
- **Ease of Use.** Simple configuration and maintenance with a secure web interface that allows for convenient setup and management. PC configuration software has been eliminated.
- **Seamless Integration.** Bump-in-the-wire design simplifies security retrofit of existing serial communications systems. Upgrade existing modems and radios to crypto-modems and crypto-radios.
- **Flexible Network Architectures.** The SEL-3025 SCADA Shield is ideally suited for point-to-point, multidrop, and many-to-many networks.
- **Syslog.** Log events with Syslog for consistency, compatibility, and centralized collection.
- **User-Based Access Control.** Strong access control and individual user accountability.
- **Reliability.** The SEL-3025 SCADA Shield is built for availability, hardened for the substation, and carries a ten-year warranty.

Product Overview

The SEL-3025 SCADA Shield is a bump-in-the-wire device that adds strong cryptographic security to serial communications links. It is designed for use on point-to-point and multidrop SCADA networks, and many-to-

many configurations as seen in remote engineering access installations where multiple users need access to the same devices.

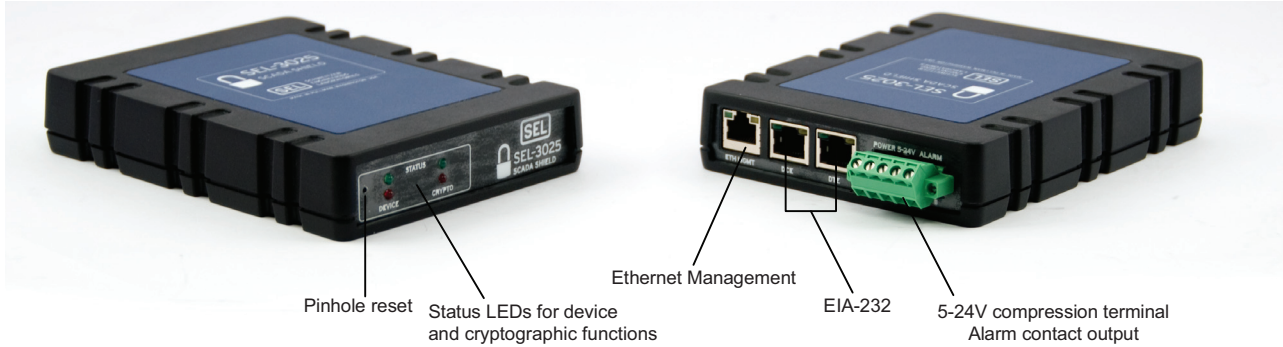


Figure 1 SEL-3025 SCADA Shield Functional Overview

The SEL-3025 SCADA Shield includes a cryptographic function to provide data authentication and optional encryption through the Secure SCADA Communication Protocol (SSCP). The SEL-3025 SCADA Shield ensures that messages are not forged, modified, spliced, reordered, or replayed. The SEL-3025 SCADA Shield also prevents unauthorized device access by rejecting all communications session requests from sources that cannot pass cryptographic session authentication. *Figure 2* shows a typical SCADA connection where a

master device retrieves data from a remote device over an untrusted communications channel. Publicly accessible channels, such as a leased phone circuit, a dial-up connection, or a radio link, are considered to be untrusted communications channels. Unauthorized individuals could alter the data these media carry. An attacker could also access the channel and inject malicious data to force an undesirable action, such as an unauthorized breaker operation.

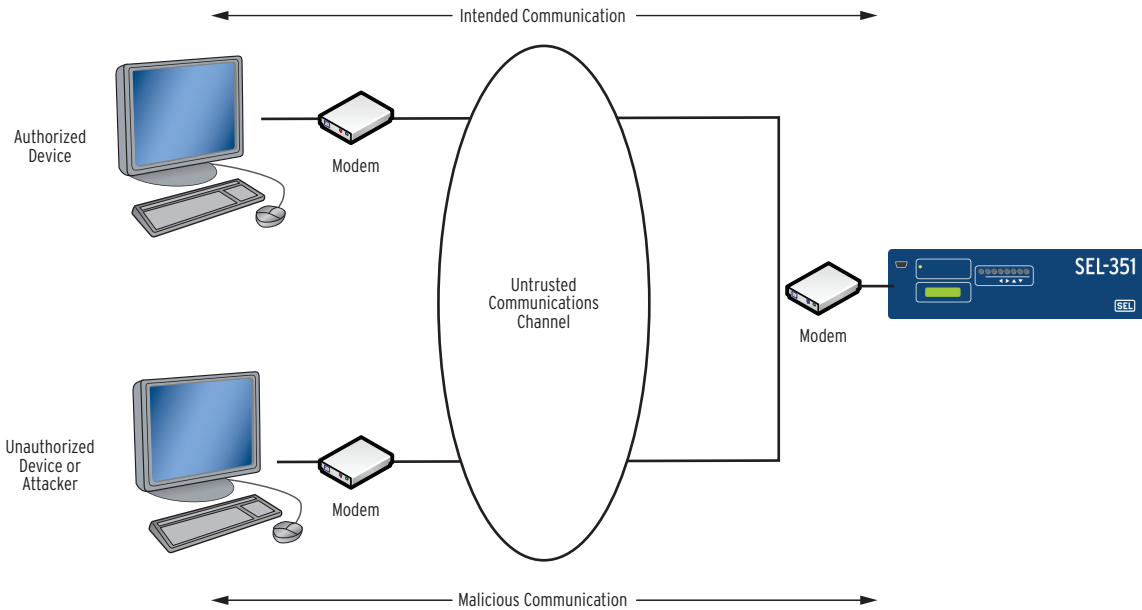


Figure 2 Typical SCADA Communications Channel

Figure 3 shows the SCADA communications link now secured by two SEL-3025 SCADA Shield transceivers. Install the SEL-3025 SCADA Shield between the master device and untrusted communications path at the master location and install a peer SEL-3025 SCADA Shield between the remote device and untrusted communi-

tions path at the remote location to provide a secure communications link over an untrusted communication channel. With the SEL-3025 SCADA Shield, legitimate communication still flows seamlessly between the master and remote devices. The transceivers block all unauthorized access to the protected master and remote IEDs.

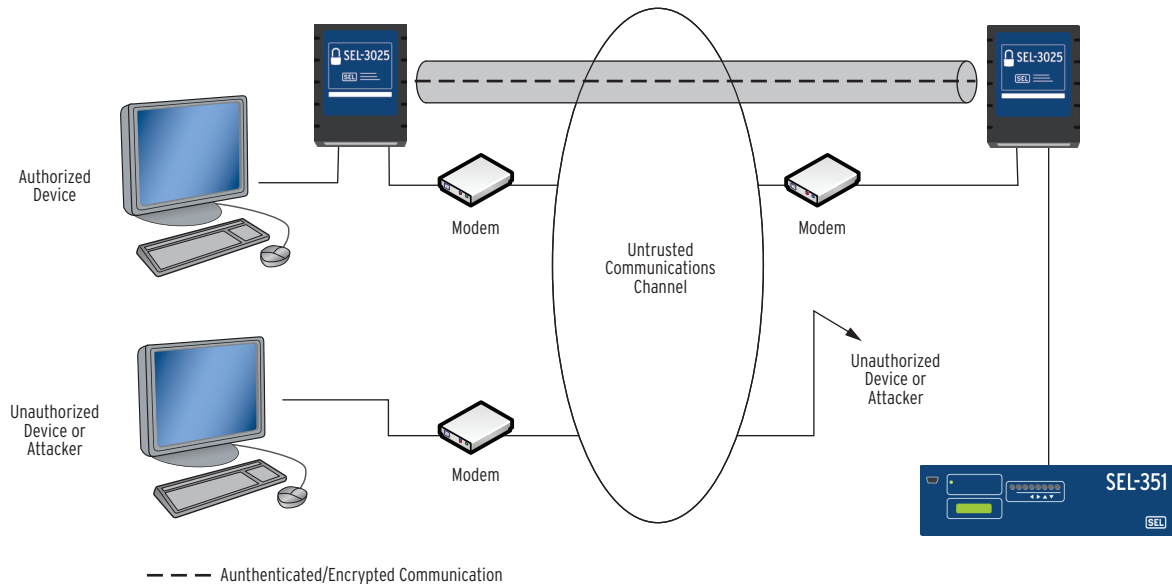


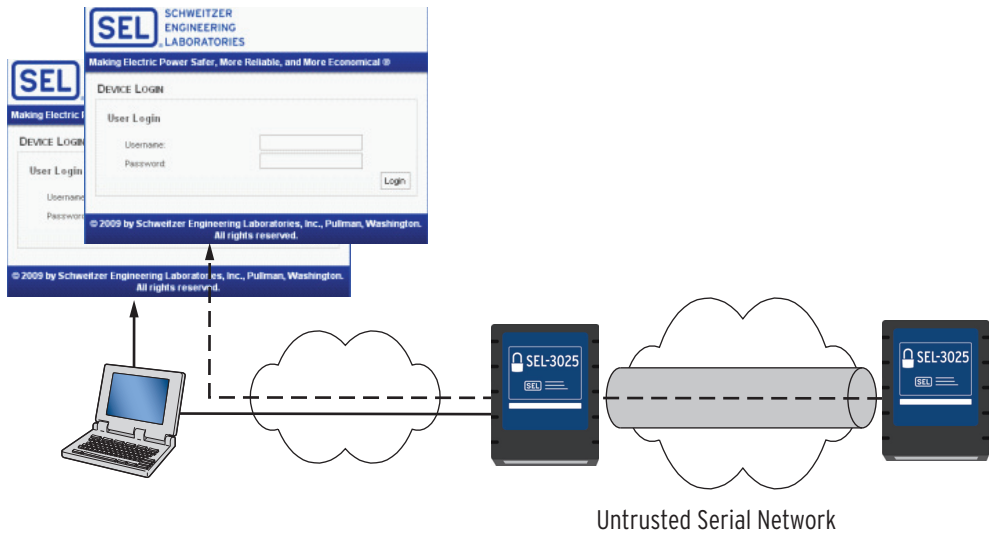
Figure 3 Secure SCADA Communications Channel

The SEL-3025 SCADA Shield consists of two serial communications ports referred to as the local interface (DCE) and the remote interface (DTE). The local interface connects to a device that requires data protection, e.g., the SCADA master or RTU. The local interface exchanges data between the protected device and the SEL-3025 SCADA Shield without cryptographic protection. The remote interface connects to an untrusted channel, such as a modem connected to a leased phone line or network connection device. The remote interface exchanges cryptographically protected data between the local and remote SEL-3025 SCADA Shield. The SEL-3025 provides the authentication and encryption through the SSCP protocol.

The SEL-3025 SCADA Shield incorporates an Ethernet port, which is used to access the secure operator web interface. The operator interface secures communication

with HTTPS running Transport Layer Security (TLS) Version 1. Each SEL-3025 SCADA Shield holds a server-side X.509 certificate to authenticate itself to incoming session requests while the user authenticates through an individually assigned username and password. This establishes a mutually authenticated connection.

This secure operator interface allows system operators to monitor the local and remote interface channel health and to program system parameters of the device without removing the SEL-3025 SCADA Shield from service or interrupting data transfer operations. This user interface also allows operators to monitor channel health and to program system parameters of any other trusted SEL-3025 SCADA Shield devices on the same serial network through a Remote Management Client as seen in Figure 4.



----- · Authenticated/Encrypted Communication

Figure 4 Nonintrusive HTTPS and Remote Management Client

Applications

The SEL-3025 SCADA Shield is ideally suited for point-to-point, multidrop, and many-to-many networks.

Point-to-Point

Figure 5 shows typical point-to-point applications including radios, dial-up modems, fiber-optic modems, and cellular modems. The SEL-3025 SCADA Shield transceivers cryptographically authenticate to protect all data between the two end points. The SEL-3025 SCADA Shield also prevents unauthorized access to either end point by rejecting all session requests that are not initiated by the authorized source.

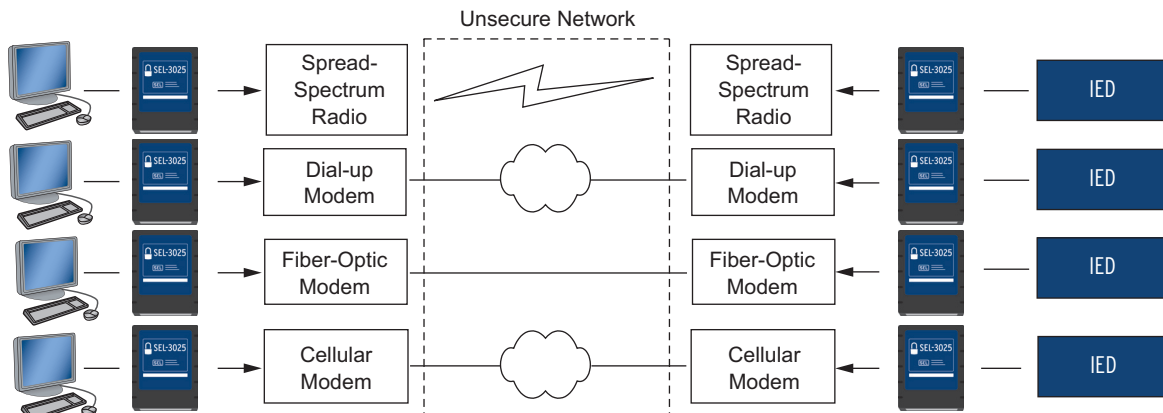


Figure 5 Point-to-Point Applications

Multidrop

Many common SCADA systems are configured in a multidrop network architecture in which several devices share a channel. On such a channel, the communications protocol must be designed to avoid collisions and transmission errors that occur when multiple devices

attempt to transmit on the shared channel at the same time. Multidrop SCADA systems employ a master device to coordinate the communication by periodically requesting data from and sending control commands to RTUs or IEDs. These master-initiated polling cycles are designed to avoid collisions on the shared transmission channel.

The SEL-3025 SCADA Shield is specifically designed to operate well in multidrop architectures. In *Figure 6*, SEL-3025 SCADA Shield devices are installed at the master and remote sites. The master cryptographic transceiver coordinates the exchange of session keys

with each remote cryptographic transceiver in the system. This coordinated exchange of session keys avoids data collisions while ensuring that a unique cryptographic key authenticates and protects each connection.

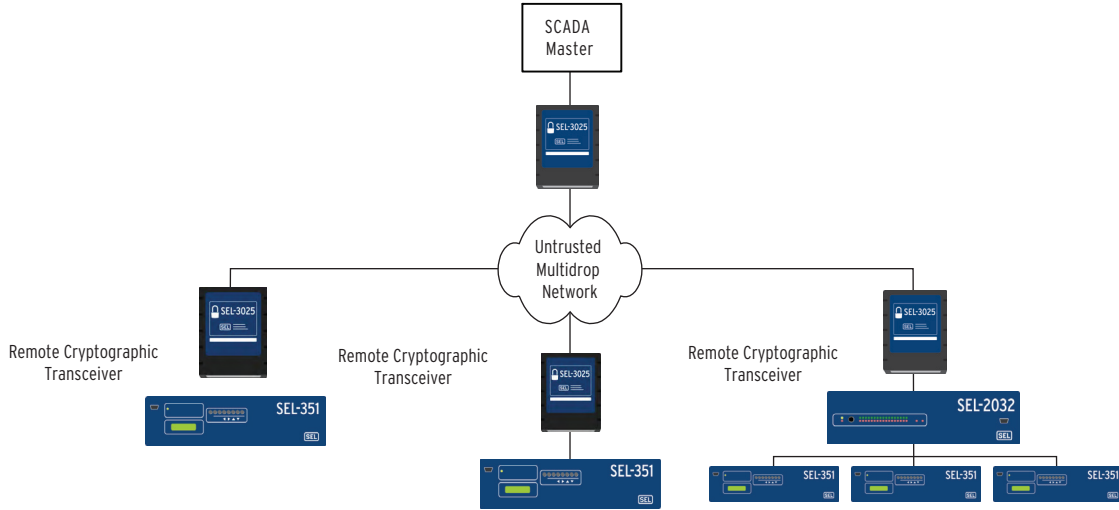


Figure 6 Multidrop Application

Many-to-Many

Many-to-many network structures are used when there are many users with authorized access to many different end points. One session can be established between a

user and end point at a given time. Once a user connects with an end point device, the SEL-3025 SCADA Shield performs as described in a point-to-point application. User-based accounts are used to provide individual accountability for actions performed on each device.

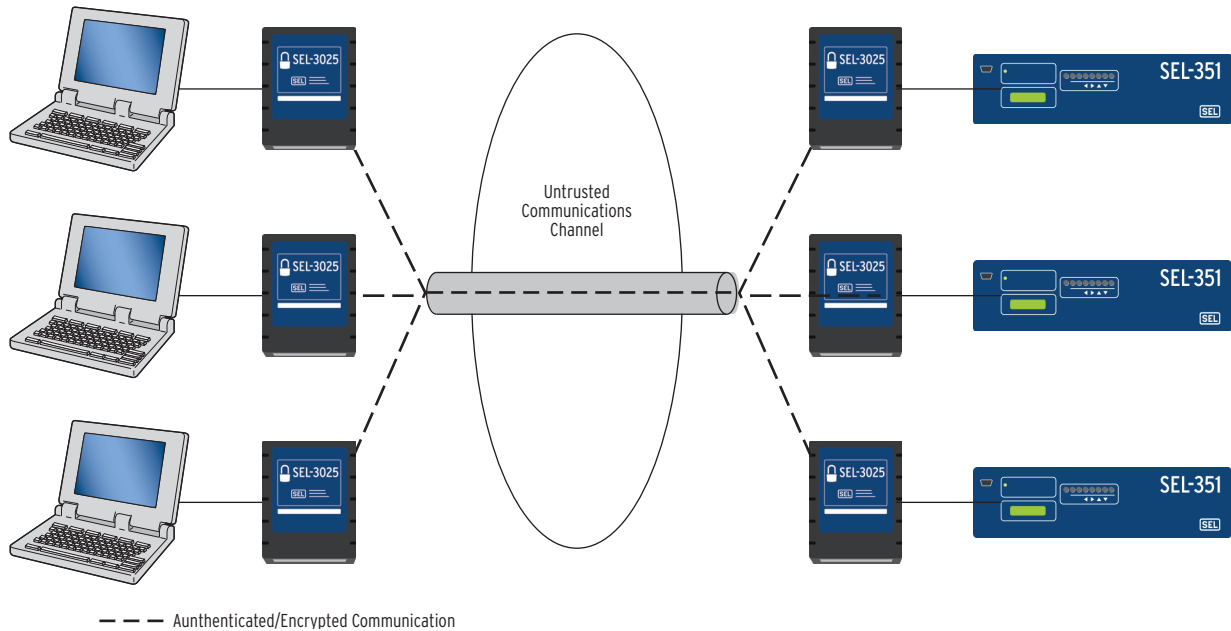


Figure 7 Many-to-Many Application

Secure SCADA Communication Protocol (SSCP)

SSCP is a cryptographic protocol used to authenticate and encrypt information exchanged over untrusted communication channels. SCADA messages are encapsulated in SSCP packets, which are then sent over the communications path to the remote SEL-3025 SCADA Shield specified in the DESTINATION field of the SSCP packet header. The remote SEL-3025 SCADA Shield validates the received SSCP packet and extracts the data to be sent to the attached device (IED, RTU,

PLC, etc.). Unauthenticated packets are logged and reported as errors, and the command in the payload is not passed on to the protected device. This prevents a malicious user from passing unauthorized commands to the remote device attached to the SEL-3025 SCADA Shield.

All SSCP packets start with the same 10-byte header format, as shown in *Table 1*.

Table 1 SSCP Header Format

0	1	2	3	4	5	6	7	8	9
SYNC TOKEN		VERSION	DESTINATION		SOURCE		PAYLOAD TYPE	LENGTH	

SYNC TOKEN: The Synchronization Tokens are the leading two bytes of all SSCP packets. The two bytes are defined as 0x16 and 0x75 to signal the start of an incoming SSCP packet.

VERSION: The VERSION field holds the version of the SSCP protocol being used. Currently, 1 is the only version.

DESTINATION: The DESTINATION field contains the 2-byte SSCP address of the device that will receive the packet.

SOURCE: The SOURCE field contains the 2-byte SSCP address of the device sending the packet.

PAYLOAD TYPE: The 1-byte PAYLOAD TYPE field specifies the type of the packet and indicates the type of payload to expect. Valid payload types are listed in *Table 2*.

LENGTH: The 2-byte LENGTH field specifies the size of the packet in bytes, not including the 10-byte SSCP header.

Table 2 SSCP Payload Types

Value	Payload Type
0x01	Data
0x02	Session Establish Request
0x03	Authentication Challenge
0x04	Authentication Response
0x05	Preshared Key Exchange
0x06	Diffie-Hellman Key Exchange
0x07	Close
8–199	Reserved
200–255	Vendor Defined

A keyed HMAC is used by the SSCP protocol to authenticate communication between devices. The HMAC is appended to normal data messages and other SSCP-specific packets, which allows the receiving device to authenticate each packet in a SSCP communication session to ensure authenticity of the data as well as the source. The receiving device must “hold back” the message before sending to the protected device because the device must receive the message and associated authentication information in its entirety to verify message authenticity and data integrity. This incurs a latency that is determined by the length of the message and the algorithm used to generate the HMAC. HMACs can be truncated to reduce latency at the cost of a less secure communications channel.

Table 3 shows a typical SSCP data packet.

Table 3 SSCP Data Packet Format

0-9	10	11	12	13	14
SSCP Header	Data Type	Sequence Number		Data (Variable Length)			HMAC (Variable Length)		

Encryption is used optionally in SSCP communication to provide data confidentiality. SSCP supports AES-128 and AES-256 for encryption in AES CTR mode. Data authenticity and integrity are provided through SHA-1 and SHA-256 cryptographic hashed message authentication code (HMAC) algorithms.

SSCP communication follows this sequence:

- Session Establish Request (Slave device only)
 - A Master device initiating a session begins with a Key Exchange (Step 4).
- Authentication Challenge

- Authentication Response
- Key Exchange
- Data
- Close

Guideform Specification

When using SEL-3025 SCADA Shield the following features shall be available.

- **Cryptographic Algorithms.** The SSCP protocol employs SHA-1 and SHA-256 for authenticity and integrity. AES-128 and AES-256 provide the optional data encryption.
- **Point-to-Point, Multidrop, and Many-to-Many Configuration.** The device shall be capable of operating in point-to-point, multidrop, and many-to-many network configurations.
- **Nonintrusive Monitoring and Setting.** The device shall provide an Ethernet interface to the HTTPS management port. The management port will be used for configuration settings and monitoring, and will be protected with encryption and authentication algorithms.
- **User-Based Accounts.** The SEL-3025 SCADA Shield employs a user-based account structure.
- **FIPS-Compliant Design for Cryptographic Modules.** The SEL-3025 shall meet FIPS 140-2 Security Level 2 criteria.
- **Warranty.** The device shall have a minimum 10 year worldwide warranty.

Specifications

Indicators

Device Status:	Green and Red LEDs
Crypto Status:	Green and Red LEDs

Solid-State Output

100 mA continuous	
250 Vdc or 120 Vac Operational Voltage	
Maximum On Resistance:	50 Ω
Minimum Off Resistance:	10 M Ω
Insulation:	1500 Vdc
Wiring size:	14 AWG Max. 26 AWG Min. 0.4 mm Min. Insulation 105°C, 250 V Min.

Cryptographic Protocols

Authentication:	SHA-1, SHA-256
Encryption:	AES-128, AES-256
Key Exchange:	Diffie Hellman
Management:	HTTPS, using X.509 certificates

User-Based Accounts

Maximum Users:	32
Maximum Password Length:	128
Password Set:	All printable ASCII characters
User Roles:	Administrator, User Manager, Engineer, Monitor

Syslog

- Storage for 2048 local Syslog messages.
- Support for Syslog forwarding to two remote Syslog servers.

Serial Ports

Connectors:	RJ45 Female (DTE) RJ45 Female (DCE)
Data Rate:	1200 bps to 115200 bps
Interface:	EIA-232

Ethernet Port

Connector:	RJ45 Female 10/100BASE-T
------------	-----------------------------

Power Requirements

+5 to +24 Vdc:	<5 W
----------------	------

Operating Temperature Range

-40°C to +85°C (-40° to +185°F)	
0 to 95% humidity (noncondensing)	

Dimensions

Height:	2.90 cm (1.14 in.)
Width:	11.43 cm (4.5 in.)
Depth:	16.22 cm (6.39 in.)

Type Tests

Electromagnetic Compatibility

Radiated Emissions:	IEC 60255-25:2000
---------------------	-------------------

Electromagnetic Compatibility Immunity

Electrostatic Discharge:	IEC 60255-22-2:2008 IEC 61000-4-2:2006 Severity Level: 4 (air discharge)
--------------------------	--

Electrical Fast Transient/ Disturbance:	IEC 60255-22-4:2008 IEC 61000-4-4:2004 Severity Level: 4 I/O signal, data, control lines: 2 kV, 5 kHz
--	---

Radio Frequency

Interference: IEC 60255-22-3:2007
IEC 61000-4-3:2006
Severity Level: 10 V/m
ANSI/IEEE C37.90.2-2004
Severity Level: 35 V/m

Environmental Tests

Cold: IEC 60068-2-1:2007
Test Ad: 16 hr at -40°C

Dry Heat: IEC 60068-2-2:2007
Test Bd: 16 hr at +85°C

Damp Heat, Cyclic: IEC 60068-2-30:2005
93% RH, 25° to 55°C, 6 cycles

Shock Resistance: IEC 60255-21-2:1988
Bump Test, Class 1
Shock Withstand, Class 1
Shock Response, Class 2

Vibration Resistance: IEC 60255-21-1:1988
Vibration Endurance, Class 1
Vibration Response, Class 2

Max. Altitude: 2000 m

Certifications

ISO: Device designed and manufactured using ISO 9001 certified quality program.

Listings: CE Mark
UL 294, 1076, 1610 pending

FIPS: 140-2 Level 2 (pending)

Warranty

10 years

© 2010 by Schweitzer Engineering Laboratories, Inc. All rights reserved.

All brand or product names appearing in this document are the trademark or registered trademark of their respective holders. No SEL trademarks may be used without written permission. SEL products appearing in this document may be covered by US and Foreign patents.

Schweitzer Engineering Laboratories, Inc. reserves all rights and benefits afforded under federal and international copyright and patent laws in its products, including without limitation software, firmware, and documentation.

The information in this document is provided for informational use only and is subject to change without notice. Schweitzer Engineering Laboratories, Inc. has approved only the English language document.

This product is covered by the standard SEL 10-year warranty. For warranty details, visit www.selinc.com or contact your customer service representative.

SCHWEITZER ENGINEERING LABORATORIES

2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Phone: +1.509.332.1890 • Fax: +1.509.332.7990
Internet: www.selinc.com • E-mail: info@selinc.com

