SEL-3025 Serial Shield
Serial Cryptographic Transceiver

Secure SCADA Communication

The SEL-3025 Serial Shield®, an EIA-232 bump-in-the-wire serial cryptographic transceiver, protects meters, protective relays, programmable logic controllers (PLCs), remote terminal units (RTUs), and computers from unauthorized access, control, eavesdropping, and malicious attack by authenticating and encrypting all serial data communications.

The SEL-3025 is ideal for protecting dial-up connections with identity-based access control.

Major Features and Benefits

- **Strong Protection for Serial Links.** Apply the SEL-3025 with all standard point-to-point, multidrop, and many-to-many serial communication architectures. The SEL-3025 comes preconfigured for quick DNP3, Modbus® RTU, Conitel, Redac, Tejas, and Van-Comm setting, and it secures all other byte-oriented data through custom settings.
- **FIPS 140-2 Level 2 Validated (Historical) Cryptographic Serial Protocols.** Match system requirements to the appropriate level of protection with two options: full message authentication with encryption or session authentication and streaming encryption. Note that current FIPS certificates are marked as historical. SEL is currently undergoing the FIPS revalidation process for both cryptographic protocols.
  - **Message authentication with encryption.** Secure SCADA Communication Protocol (SSCP) is best for engineering access. Order the SSCP module when you need to authenticate every data packet on your serial link. SSCP can also provide strong encryption through the use of NIST-approved Advanced Encryption Standard (AES) encryption with strong 128-bit or 256-bit keys.
  - **Low-latency streaming encryption.** Streaming Encryption Protocol (SEP) is best for SCADA and real-time protection. Order SEP when you are protecting data for systems, such as SCADA, metering, and protection, that require time-critical communications.
- **Seamless Integration.** Retrofit existing serial communications systems easily with the SEL-3025 simple bump-in-the-wire design, or upgrade existing modems and radios to cryptomodems and cryptoradios.
- **Individual User Accountability.** Secure all your dial-up modems with identity-based access controls and reports that you can manage centrally.

- **Web-Based Configuration.** Set up and manage configuration of both local and remote units with a secure web interface that allows for intuitive and simple setup and management through the use of a web browser.
- **Import/Export Configuration File.** Quickly generate back-up configuration files and restore settings with a secure file transfer.
- **User-Based Access Control.** Enforce strong access controls and individual user accountability with user-based security for the web-based management interface.
- **Central Management.** Centrally manage the SEL-3025 through ACSELERATOR QuickSet® SEL-5030 Software or take the next step and fully automate central management through ACSELERATOR TEAM® SEL-5045 Software.
- **Syslog.** Log events with Syslog for consistency, compatibility, and centralized collection.
- **Reliability.** The SEL-3025 is built for availability, hardened for the substation, and carries a 10-year warranty.

Product Overview

The SEL-3025 Serial 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 links, multidrop SCADA networks, and many-to-many dial-up configurations often found in remote engineering access installations where multiple users need access to the same devices.

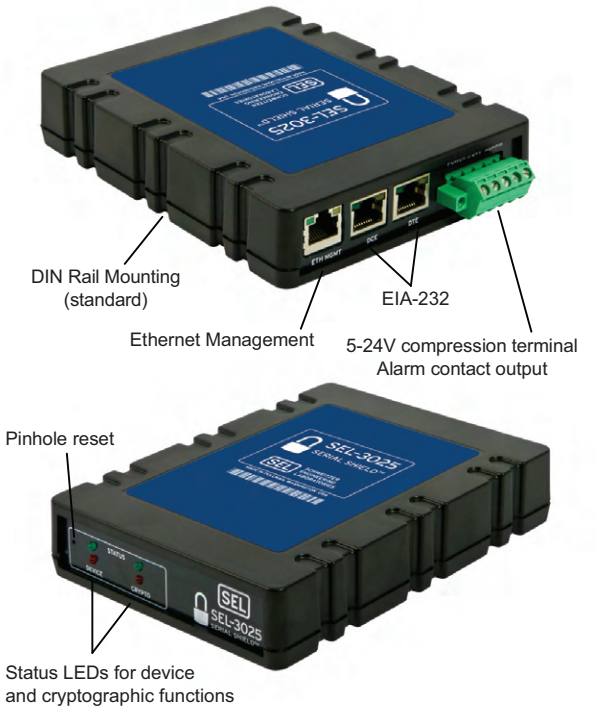

Figure 1 SEL-3025 Serial Shield Functional Overview

The SEL-3025 Serial Shield has 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 (the SCADA master or RTU, for example). The local interface exchanges data in the clear (without cryptographic protection) between the protected device and the SEL-3025 Serial Shield. The remote interface connects to an untrusted channel, such as a modem connected to a leased phone line or other communications equipment. The remote interface exchanges cryptographically protected data between the local and remote SEL-3025 Serial Shield.

Two Encryption Options Protect Critical Data

SEL offers two encryption options for the best combination of security with the least latency: Secure SCADA Communication Protocol (SSCP) for stronger message integrity assurance, and Streaming Encryption Protocol (SEP) for least latency in real-time applications.

When to Choose Secure SCADA Communication Protocol (SSCP)

Choose the Secure SCADA Communication Protocol (SSCP) to provide the highest level of protection data integrity and authenticity when transmission latency would not be a problem. SSCP protects against spoofed, altered, spliced, reordered, or replayed data with strong data authentication as well as optional AES-128 or AES-256 data encryption for protection against eavesdropping. SSCP also prevents unauthorized device access by rejecting all communications session requests from sources that cannot pass cryptographic session authentication. *Figure 2* shows a typical engineering access connection where an engineering workstation retrieves data from a remote device over an untrusted communications channel. We can consider publicly accessible channels, such as a leased phone circuit, a dial-up connection, or a radio link, untrusted communi-

cations channels. An attacker could access the channel and inject malicious data or replay old data to force an unwanted action, such as an unauthorized breaker operation, by connecting to the remote modem.

Figure 3 shows the engineering communications link now secured by two SEL-3025 Serial Shield transceivers. Install the SEL-3025 Serial Shield between the master device and untrusted communications path at the master location and install a peer SEL-3025 Serial Shield between the remote device and untrusted communications path at the remote location to provide a secure communications link over an untrusted communications channel. With the SEL-3025 Serial 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. The SSCP protocol is a byte-oriented protocol that offers the strong encryption and message authentication features necessary for engineering access.

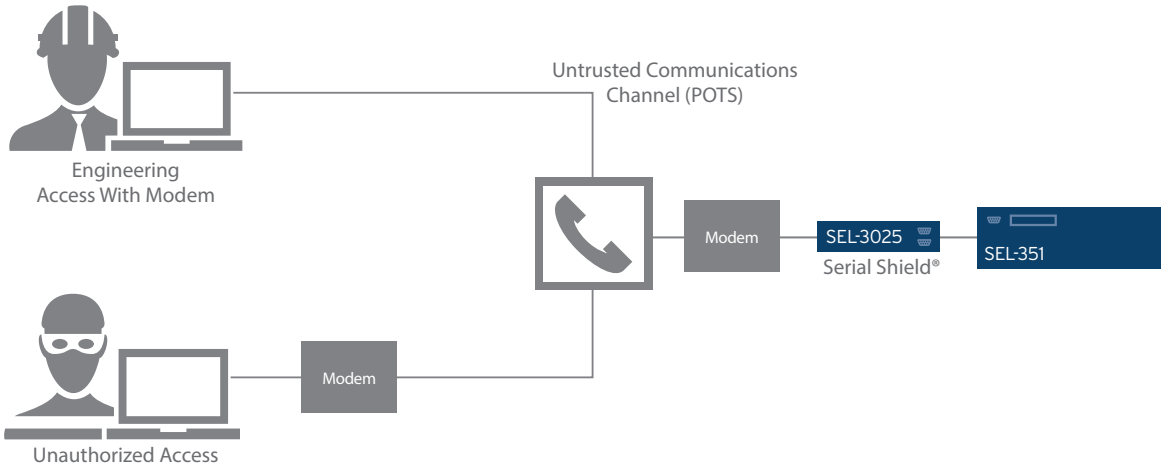

Figure 2 Typical Engineering Access Communications Channel

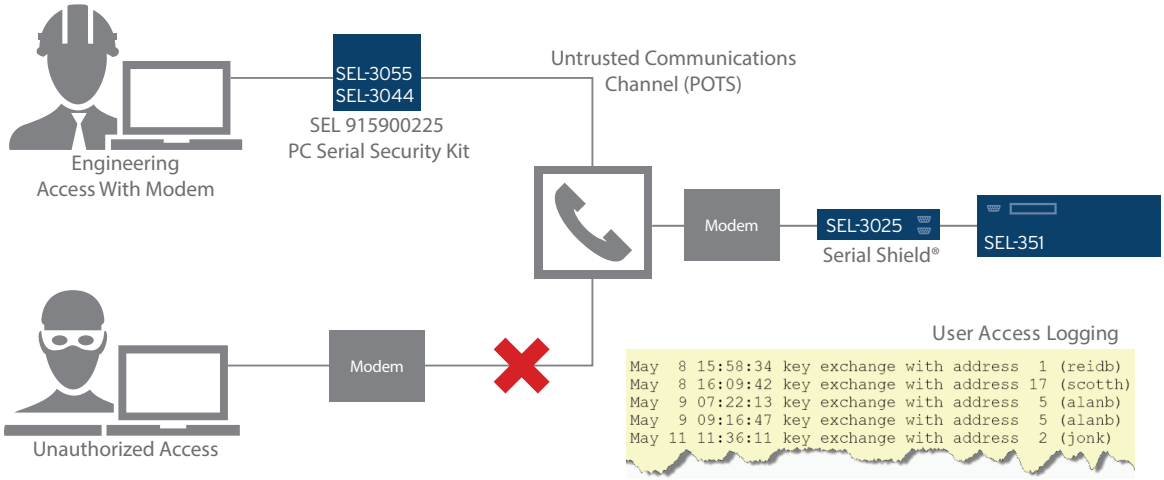

Figure 3 Secure SCADA Communications Channel

When to Choose Streaming Encryption Protocol (SEP)

Choose the SEL-3025 Serial Shield streaming encryption option for real-time applications where low latency is important. Authentication of communicating stations occurs during key negotiation, and establishment of an AES-256 stream cipher then protects the stream. This protocol is better suited to SCADA and real-time protection applications where low latency is necessary.

The *Figure 4* shows a line protection application with two SEL-421 relays communicating MIRRORED BITS® real-time protection information through an untrusted network. Install the SEL-3025 Serial Shield between the SEL-421 and the multiplexer at Station 1, and install a matching SEL-3025 Serial Shield between the SEL-421 and the multiplexer at Station 2 to protect the data link from tampering and eavesdropping with low-latency streaming encryption.

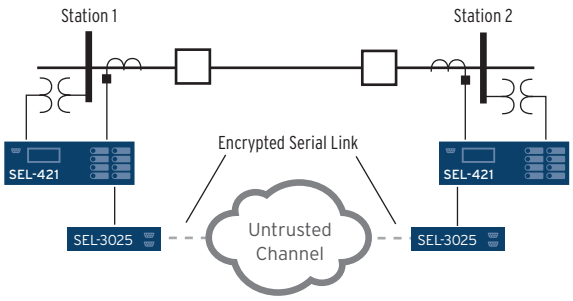

Figure 4 Real-Time Protection Data Protected With Streaming Encryption

Setup and Management

The SEL-3025 Serial Shield incorporates an Ethernet port that you can use to access the web interface for configuration and management. The web interface uses Transport Layer Security (TLS) to secure communications with HTTPS. Each SEL-3025 Serial Shield holds a server-side X.509 certificate to authenticate itself to incoming session requests, while users authenticate through individually assigned usernames and passwords. 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 Serial Shield from service or interrupting data transfer operations. The SEL-3025 can also extend administrative access to remote SEL-3025 units reachable on the same serial network through use of the remote management client feature, as seen in *Figure 5*.

When the Remote Management Client is in use, the SEL-3025 Serial Shield suspends serial traffic during the administrative session.

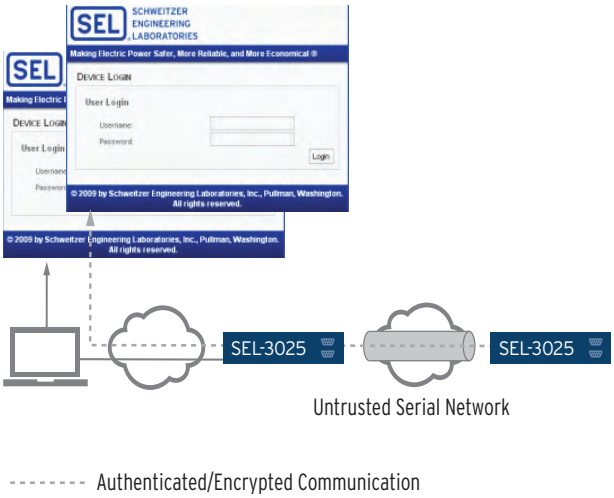

Figure 5 Nonintrusive HTTPS and Remote Management Client

Applications

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

Point-to-Point

Figure 6 shows typical point-to-point applications including radios, dial-up modems, fiber-optic modems, and cellular modems. The SEL-3025 Serial Shield transceivers cryptographically authenticate to protect all data between the two endpoints. The SEL-3025 Serial Shield also prevents unauthorized access to either endpoint by rejecting all session requests that the authorized source does not initiate.

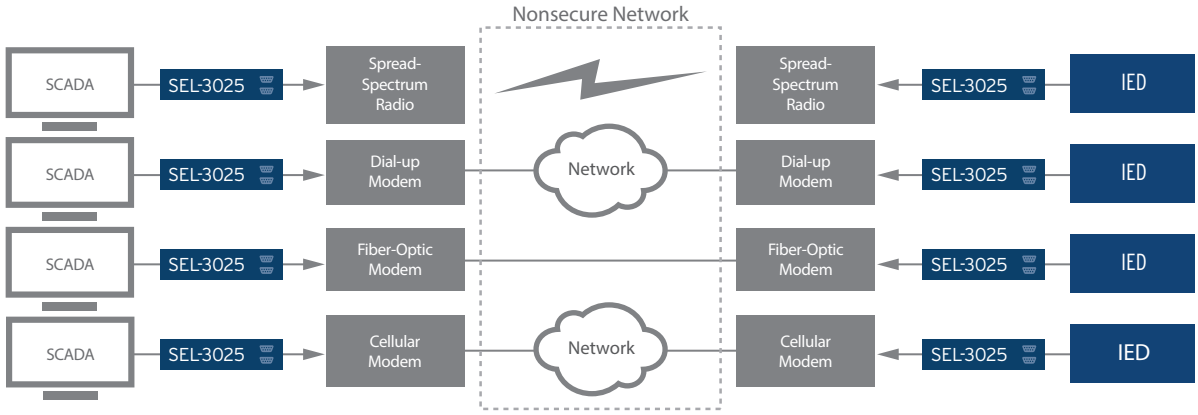

Figure 6 Point-to-Point Applications

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 Serial Shield is specifically designed to operate well in multidrop architectures. In *Figure 7*, SEL-3025 Serial 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.

Many-to-Many

Many-to-many network structures are applicable when there are many users with authorized access to many different endpoints. One session can be established between a user and endpoint at a given time. Once a user connects with an endpoint device, the SEL-3025 Serial Shield performs as described in a point-to-point application. User-based accounts provide individual accountability for actions each device performs.

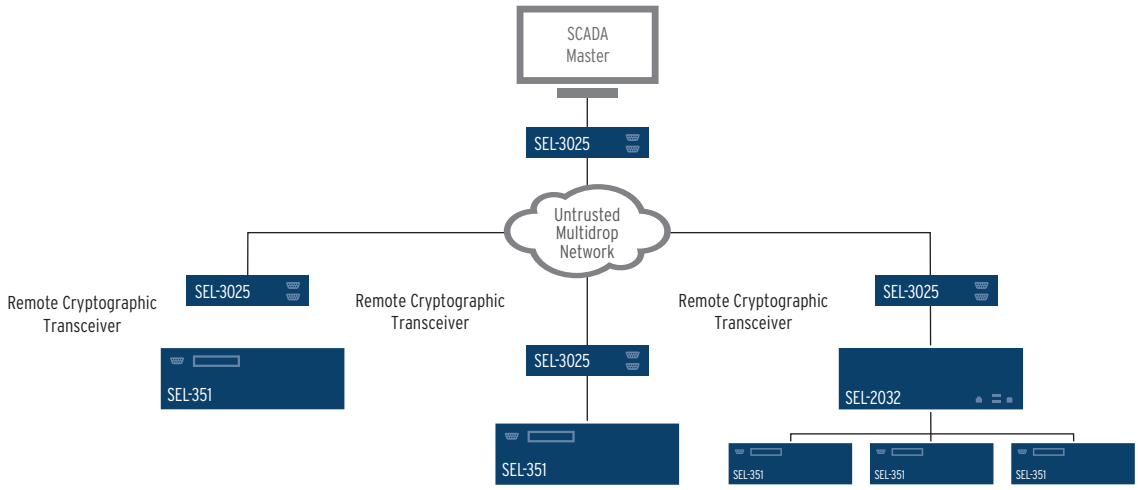

Figure 7 Multidrop Application

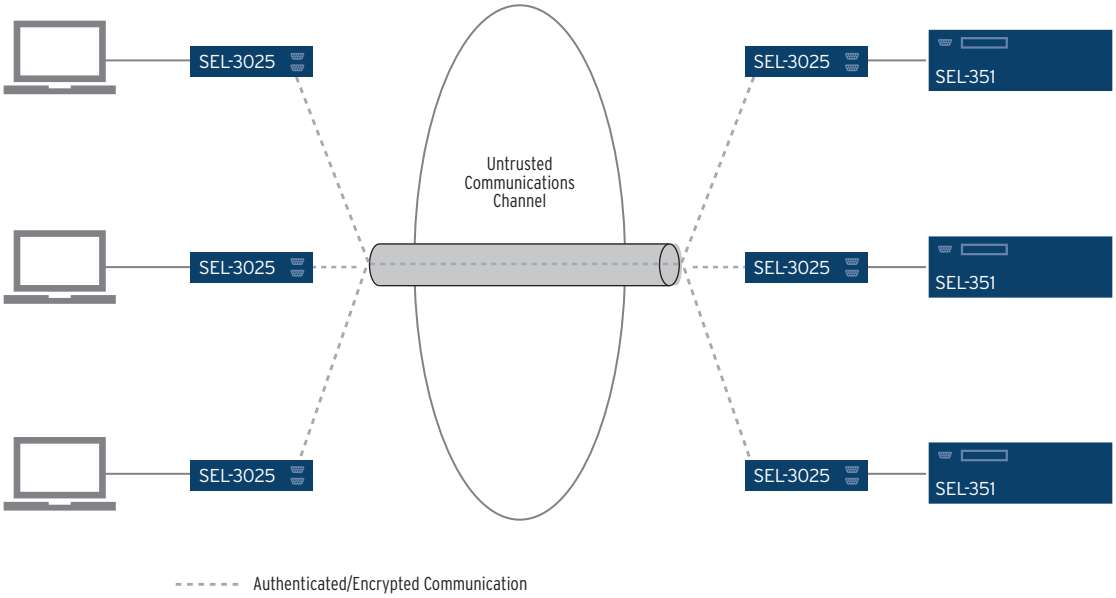

Figure 8 Many-to-Many Application

Secure SCADA Communication Protocol (SSCP)

SSCP is a cryptographic protocol that we can use to authenticate and encrypt information exchanged over untrusted communications channels. SCADA messages are encapsulated in SSCP packets, which are then sent over the communications path to the remote SEL-3025 Serial Shield specified in the DESTINATION field of the SSCP packet header. The remote SEL-3025 Serial Shield validates the received SSCP packet and extracts the data to be sent to the attached device (IED, RTU, PLC, etc.). The SEL-3025 logs and reports as errors any unauthenticated packets and blocks passage of the command in the payload on to the protected device. This prevents a malicious user from passing unauthorized commands to the remote device attached to the SEL-3025 Serial Shield.

Key Management

- System key (128 bits or 256 bits): Your information technology (IT) or system administrator sets the system key. Use the system key to encrypt and securely transmit unique session keys (see below). The system key also provides a cryptographic authentication mechanism for rejecting session requests by unauthorized SEL-3025 devices.
- Session key (128 or 256 bits): Session keys authenticate and can optionally encrypt user data prior to transmission. The SEL-3025 produces session keys at system startup and periodically during sessions. The SEL-3025 uses an FIPS 186-2 compliant procedure, incorporating an integrated physical random number generator (RNG) and a statistical data-whitening algorithm, to generate session keys. Session keys are purely random and are not linked to the system key. The use of periodically changed session keys limits the amount of data that are encrypted with a single key value, thus strengthening the system against cryptanalytic attack. Encryption of the session keys, through use of the system key, occurs prior to exchange of the session keys between SEL-3025 transceivers.

Device Security

- The SEL-3025 cryptography module incorporates a hardware RNG and an FIPS-approved data whitener to guarantee that session keys contain their full bit length of entropy (i.e., complete randomization). This guarantees that encoded messages are protected by the full cryptographic strength of the specified key length.
- Multilevel password authentication defines user security roles.
- Only authorized users using the secure operator interface and SEL configuration software can change system keys.
- If necessary, users can reset the entire device. This allows users to reinstall the system key, should the security parameters need to change as a result of IT security procedures or loss of the programmed system key value. Note: This process requires physical access to the SEL-3025; you cannot perform this process remotely.

Table 1 SSCP Data Packet Format

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

Message Authentication and Latency

The SSCP protocol uses a keyed hash-based message authenticated code (HMAC) to authenticate communication between devices. The SEL-3025 appends the HMAC to normal data messages and other SSCP-specific packets to allow the receiving device to authenticate each packet in an SSCP communications session and ensure authenticity of the data as well as the source. The receiving device must "hold back" the message before sending it to the protected device; 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 depends upon the length of the message and the algorithm that generates the HMAC. It is possible to truncate HMACs to reduce latency, but this truncation comes at the cost of a less secure communications channel.

You can at your option use encryption in SSCP communication to provide data confidentiality. SSCP uses AES-128 and AES-256 for encryption in AES CTR mode. SHA-1 and SHA-256 HMAC algorithms provide data authenticity and integrity.

Streaming Encryption Protocol

The Streaming Encryption Protocol uses the Advanced Encryption Standard (AES) algorithm with a key length of 256 bits. The National Institute of Standards and Technology (NIST) has approved this algorithm as a secure means of encrypting data. The design of the SEL-3025 RNG used for key generation ensures that all $1.2 \bullet 10^{77}$ possible key values are equally likely. It is widely accepted throughout the cryptographic community that it is not realistically possible to mount a successful brute force (key guessing) attack on a 256-bit key space with technology available today.

Key Management

- System key (256 bits): Your IT or system administrator sets the system key. Use the system key to encrypt and securely transmit unique session keys (see below). It also provides a cryptographic authentication mechanism for rejecting session requests by unauthorized SEL-3025 devices.
- Session key (256 bits): Session keys encrypt all protected user data prior to transmission. The SEL-3025 produces these at system startup and periodically during sessions. The SEL-3025 uses the FIPS 186-2 compliant procedure, incorporating an integrated physical random number generator and a statistical data-whitening algorithm, to generate session keys. Session keys are purely random and are not linked to the system key. The use of periodically changed session keys limits the amount of data encrypted with a single key value, thus strengthening the system against cryptanalytical attack. Encryption of the session keys, through use of the system key, occurs prior to exchange of the session keys between SEL-3025 transceivers.

Device Security

- The SEL-3025 cryptography module incorporates a hardware RNG and an FIPS-approved data whitener to guarantee that session keys contain 256 bits of entropy (i.e., complete randomization). This guarantees that encoded messages are protected by a true cryptograph strength of 256 bits.
- Multilevel password authentication defines user security roles.
- Only authorized users using the secure operator interface and SEL configuration software can change system keys.
- If necessary, you can reset the entire device. This allows you to reinitialize the system key should the security parameters need to change as a result of IT security procedures or loss of the programmed system key value. Note: This process requires physical access to the SEL-3025; you cannot perform this process remotely.

Data Latency

The SEL-3025 provides reliable and secure data communications while minimizing the communication delays (data latency) added by the devices. *Figure 9* shows a local SEL-3025 and a remote SEL-3025 communicating over a nonsecure network. At time t_0, the local SEL-3025 begins receiving a single SCADA frame on its local interface (i.e., the local SEL-3025 begins receiving the first byte of the frame at this time). At time t_1, the remote SEL-3025 has received and finished processing the first byte of the same SCADA frame and begins transmitting the byte to the protected device attached to its local interface. The time difference, $t_1 - t_0$, represents the total communication delay introduced by inserting the two SEL-3025 transceivers into the data path. There are two sources for this introduction of latency: data buffering in the SEL-3025, and transmission of cryptographic overhead introduced by the SEL-3025 (cryptographic headers at the beginning of each frame).

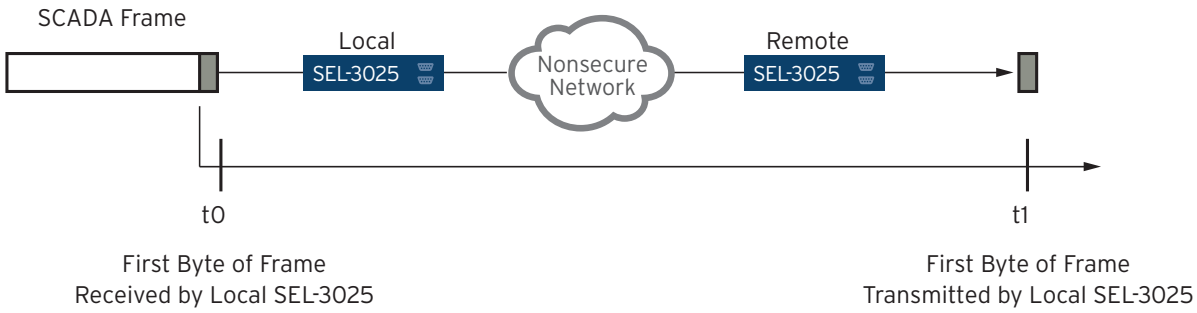

Figure 9 Data Transmission Latency

The pair of SEL-3025 transceivers introduces two byte-times of latency to the communications path (one per device) as a result of buffering in the reception Universal Asynchronous Receiver/Transmitter's (UARTs). For most common SCADA protocols, the SEL-3025 will add only 3 bytes of cryptographic overhead to each frame. These two effects combine to introduce five byte times of communications latency. *Table 2* shows the approximate latency introduced by a pair of SEL-3025 transceivers for an EIA-232 configuration with a single start bit and a single stop bit.

Table 2 Communications Latency

Data Rate, BPS	Latency ($t_1 - t_0$), Milliseconds
300	167
1200	42
2400	21
4800	10
9600	5.2
19200	2.6
38400	1.3

Related Products

The 915900225 PC Serial Security Kit can be used to allow a personal computer to communicate securely with remote terminals protected by an SEL-3025. A separate data sheet is available for the 915900225.

Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

UL Recognized to UL 294 Standard for Access Control System Units-Edition 6 (File BP10155)

SSCP (SEL-3045 encryption card): an FIPS 140-2 Level 2 (historical, pending revalidation) validation certificate #1488 (consolidated certificate no. 0002)
SEP (SEL-3044 encryption card): FIPS 140-2 Level revalidation is pending
Note that current FIPS certificates are marked as historical. SEL is currently undergoing the FIPS revalidation process for both cryptographic protocols.

Indicators

Device Status:	Green and Red LEDs
Crypto Status:	Green and Red LEDs
EIA-232 Communication:	Green and Yellow LEDs
Network (TCP/IP) Communication:	Green and Yellow LEDs

Solid-State Output

100 mA continuous

250 Vdc or 120 Vac Operational Voltage

Maximum On Resistance:	50 Ω
Minimum Off Resistance:	10 MΩ
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, AES Key Wrap
Management:	HTTPS, using X.509 certificates 1024 or 2048 Secure File Transfer

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 57600 bps
Interface:	EIA-232

Ethernet Port

Connector:	RJ45 Female 10/100BASE-T

Accessories

Power Adapter/Cable:	The SEL 230-0604 power supply is designed to power the SEL-3025 from an ac source. SEL-9321 Low-Voltage DC Power Supply SEL-9322 15 Vdc Power Supply
Communications Cables:	For supporting data cables, use the SEL-5801 Cable Selector Program. Download the SEL-5801 Cable Selector Program for free at selinc.com. SEL-C609 straight-through RJ45 to 9-pin female SEL-C616 straight-through RJ45 to 9-pin male SEL-C629A null modem RJ45 to RJ45

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 Emissions

Product Specific:	IEC 60255:2013; Section 7.1 CISPR 22:2008 CISPR 11:2010
Generic	FCC CFR 47:2008; Part 15 Severity Level: Class A

Electromagnetic Compatibility Immunity

Electrostatic Discharge:	IEC 60255-26:2013; Section 7.2.3 Severity Level: 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEC 61000-4-2:2008 Severity Level: 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEEE C37.90.3-2001 Severity Level: 2, 4, 8 kV contact; 4, 8, 15 kV air

Radiated RF:	IEC 60255-26:2013; Section 7.2.4 Severity Level: 10 V/m IEC 61000-4-3:2010 Severity Level: 10 V/m IEEE C37.90.2-2004 Severity Level: 35 V/m
Fast Transient/Burst:	IEC 60255-26:2013; Section 7.2.5 Severity Level: Zone A: 4 kV at 5 kHz, 2 kV at 5 kHz on communications ports IEC 61000-4-4:2012 Severity Level: 4 kV at 5 kHz, 2 kV at 5 kHz on communications ports
Surge Withstand Capability:	IEC 60255-26:2013; Section 7.2.6 Severity Level, Zone A: 2.5 kV peak common mode, 1.0 kV peak differential mode IEEE C37.90.1-2012 Severity Level: 2.5 kV oscillatory, 4 kV fast transient waveform
Conducted RF:	IEC 60255-26:2013; Section 7.2.8 Severity Level: 10 Vrms IEC 61000-4-6:2008 Severity Level: 10 Vrms

Environmental

Cold:	IEC 60068-2-1:2007 Severity Level: 16 hours at –40°C
Damp Heat, Cyclic:	IEC 60068-2-30:2005 Severity Level: 25° to 55°C, 6 cycles, Relative Humidity: 95%
Dry Heat:	IEC 60068-2-2:2007 Severity Level: 16 hours at +85°C
Mechanical:	IEC 60255-21-2:1988 Severity Level: Class 1 – Shock Withstand, Bump, and Class 2 – Shock Response IEC 60255-21-3:1993 Severity Level: Class 2 (Quake Response) IEC 60255-21-1:1988 Severity Level: Class 1 Endurance, Class 2 Response

Performance Level for Access Control (UL 294 6th Ed.)

Model:	SEL-3025 Series
Endurance:	Level IV
Line Security:	Level III
Destructive Attack:	Level I
Power Standby:	Level I

Warranty

10 years

Notes

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
selinc.com • info@selinc.com

PDS3025-01

SEL-3025 Data Sheet

Date Code 20190228