SEL-3622

Security Gateway

Merge physical security and cybersecurity for field operations.

- Small form factor and wide temperature range for cabinet installation on distribution poles and in substation yards.

- Accelerometer, light sensor, and cable disconnect detection alert on physical tampering.

- Deny-by-default firewall and virtual private network (VPN) encryption protect all traffic in remote field cabinets.

- Multifactor authentication keeps engineering access to all devices secure.

- Embedded allowlist antivirus technology reduces zero-day virus threats.

- Best-in-class encryption and authentication of information packets is provided with four IPsec profiles to choose from, including 2022 Secure with updated cipher suites.

SEL

Key Features

Embedded Allowlist Anti-Malware

Resist known and unknown malware attacks with exe-GUARD® embedded antivirus. Powerful rootkit resistance technology, embedded Linux mandatory access controls, and process allowlisting help mitigate attacks against the gateway itself and eliminate costly patch management and antivirus signature updates.

Serial-to-Ethernet Transceiver

Expand your protocol compatibility by converting serial DNP3 and Modbus to Ethernet DNP3 Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) and Modbus TCP on the fly. Establish an Ethernet connection using Secure Shell (SSH), Telnet, raw TCP, or UDP encapsulation to create a persistent tunnel between a logical Ethernet port and a physical serial port. The device can also convert most bit-based protocols (Conitel, Tejas, Van Comm, etc.) to Ethernet to help replace analog links without disrupting existing systems.

Secure Electronic Access Point to Electronic Security Perimeters

Use the SEL-3622 Security Gateway to provide a central point of entry to one or several IEDs with user-based access controls and detailed activity logs. Log on to the SEL-3622 jump host functionality, not IEDs. Manage user accounts and group memberships centrally using Lightweight Directory Access Protocol (LDAP)-accessible systems, such as Microsoft Active Directory, or by using Remote Authentication Dial-In User Service (RADIUS). RADIUS functionality enables multifactor authentication technology, such as RSA tokens.

Enhanced Data Security With IPsec VPN

Communicate with existing IT and control systems over VPN tunnels secured with IPsec. Protect Ethernet or serial data regardless of the endpoint or recloser control vendor. IPsec on the SEL-3622 is interoperable with other Lemnos-compliant VPN endpoints.

Support for NERC CIP Requirements

The SEL-3622 provides automated IED password management and enforces complex passwords. Establish secure role-based engineering access controls that log and time-stamp all access attempts and every command entered on remote IEDs. Integrate event records into existing log management systems using Syslog.

Small Form Factor With Low Power Draw

The SEL-3622 Gateway's small form factor fits into field cabinets or other confined spaces. It supports 10–30 Vdc inputs and draws less than 5 W of power (for dual-copper configuration). The SEL-3622 Gateway's three Ethernet ports and four serial ports support a wide variety of Ethernet and serial-to-Ethernet communications configurations.

Virtual Software Client Support

Transform unsecure serial or legacy Ethernet communications on Microsoft Windows computers to cryptographically secure channels by using SEL-5827 Virtual Connect Client or SEL-5828 Virtual Port Service Software. These applications are provided free by SEL to make remote SEL-3622 ports available for existing software and terminal applications on your PC, including those using Modbus TCP/RTU. Data are secured using SSH with SEL-3622 port groups, master ports, and serial ports.

Physical Security Protections

Alert on possible malicious physical activity with physical sensor components on the SEL-3622 Security Gateway. The SEL-3622 can detect sudden movement (through an embedded accelerometer), sudden changes in visible light (through an embedded light sensor), the opening of cabinet doors (through an input sensor), and the connection and disconnection of Ethernet cables.

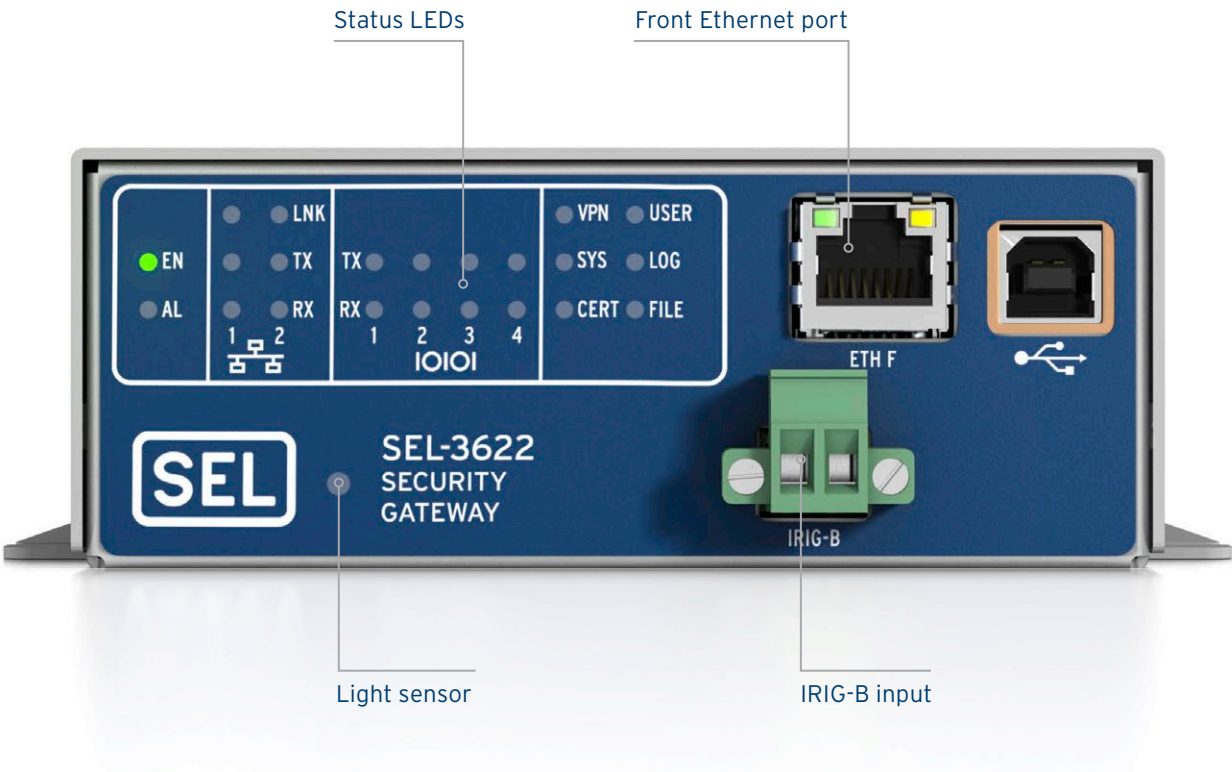### Secure Recloser Communications With MACsec

Use Media Access Control Security (MACsec) to enhance the existing cybersecurity of the SEL-651R and SEL-651RA recloser controls and reduce operation and maintenance expenses. MACsec secures Ethernet traffic (except IEC 61850 GOOSE and Parallel Redundancy Protocol [PRP] traffic) between an SEL-651R/651RA and SEL-3622 or Key Server MACsec-enabled routers/radios, providing confidential communication and maintaining message integrity between devices. Key management is automated via the MACsec Key Agreement (MKA) to simplify commissioning and improve the overall user experience.

Enterprise VPN
Concentrator

SEL-3061

Wireless Link
Secured by IPsec

SEL-651R

SEL-3061

SEL-3622

Secure all Ethernet and serial data communications with IPsec or SSH.

Product Overview

Status LEDs

Front Ethernet port

LNK

EN

AL

TX

RX

1 2

TX

RX

1   2   3   4

IOIOI

VPN USER

SYS LOG

CERT FILE

ETH F

SEL

SEL-3622
SECURITY
GATEWAY

IRIG-B

Light sensor

IRIG-B input

2 DB-9 EIA-232

Rear Ethernet ports

ETH 1   ETH 2

COM 3   COM 4

COM 1   COM 2

OUT101   IN101   POWER

2 DB-9 EIA-232/-422/-485 software-
selectable serial ports, all with IRIG-B
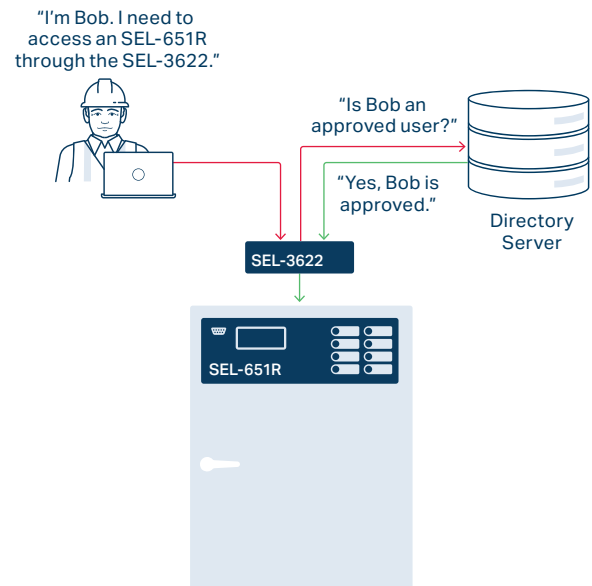
Cabinet door contact
sensor input
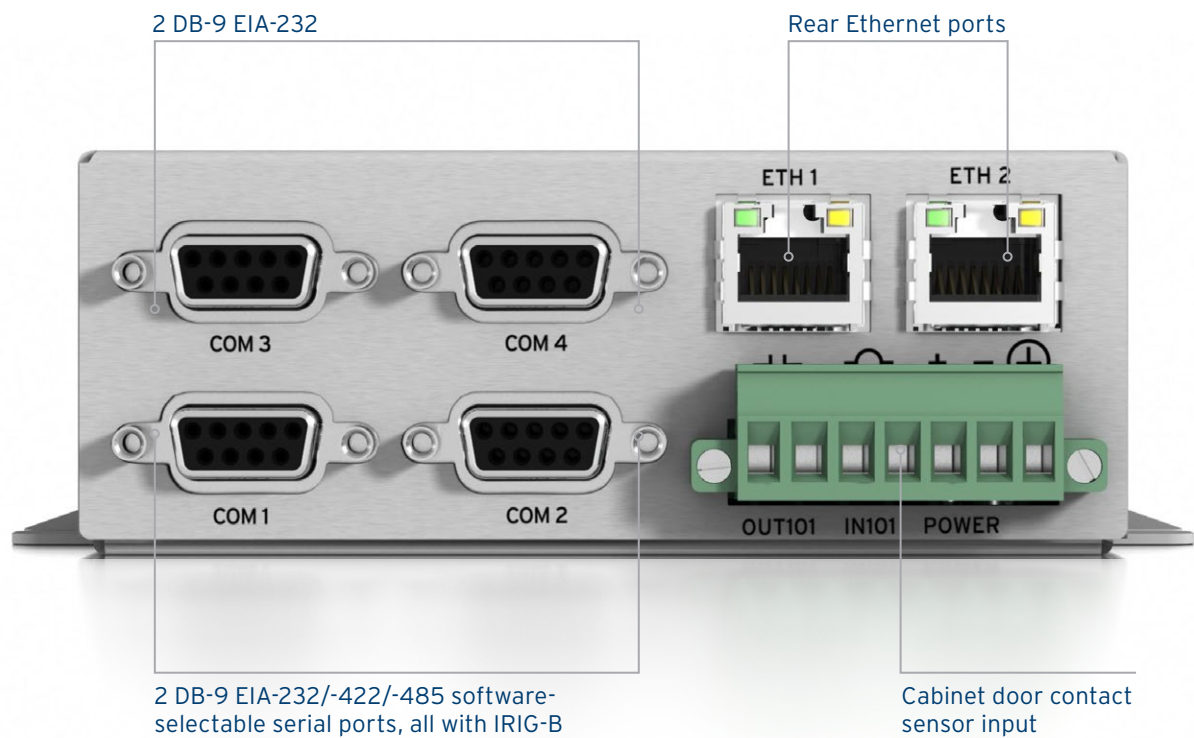
Applications

Accountability and Compliance

Integrate into existing log management systems using Syslog. Centralized log collection also means easier compliance with NERC CIP event logging rules and regulations. Use SEL-3622 proxy services to generate user command reports and to trace all actions performed on IEDs back to individual users. Log all successful or blocked connections to the firewall, and be alerted to the presence of unauthorized network communication attempts.
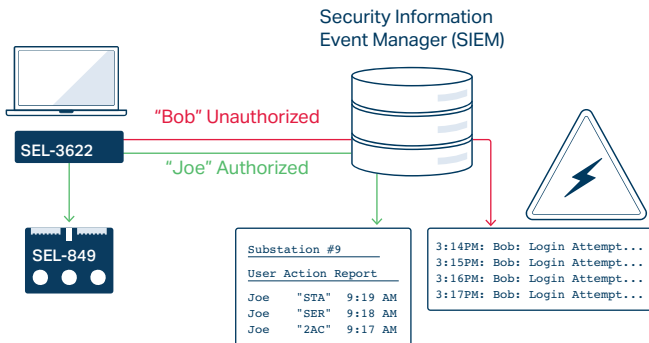
User Access Control

Query Microsoft Active Directory using LDAP or RADIUS. System administrators can easily add and remove user-based account access and authorized access levels to specific devices from a central location.

Security Information
Event Manager (SIEM)

"Bob" Unauthorized

"Joe" Authorized

SEL-3622

SEL-849

Substation #9

User Action Report

Joe   "STA"   9:19 AM
Joe   "SER"   9:18 AM
Joe   "2AC"   9:17 AM

3:14PM: Bob: Login Attempt...
3:15PM: Bob: Login Attempt...
3:16PM: Bob: Login Attempt...
3:17PM: Bob: Login Attempt...

"I'm Bob. I need to access an SEL-651R through the SEL-3622."

"Is Bob an approved user?"

"Yes, Bob is approved."
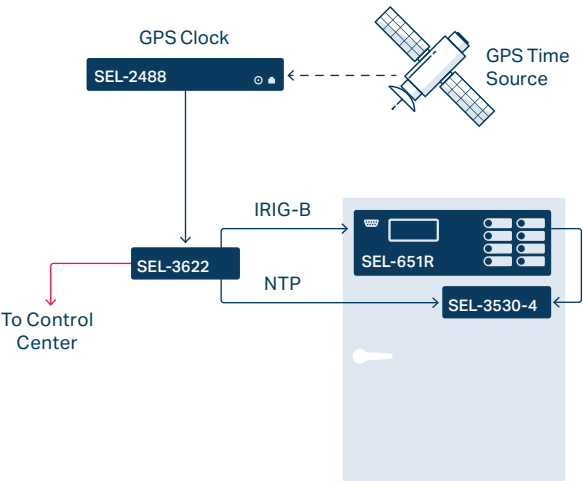
Directory Server

SEL-3622

SEL-651R

Automated IED Password Management

Manage IED passwords quickly and efficiently with SEL-3622 proxy services. Enforce strong passwords on IEDs that automatically change on a configurable schedule. Ensure that no default or weak passwords are in use on critical networks. Use the SEL Data Management and Automation (DMA) application suite to automate the collection of password change reports.
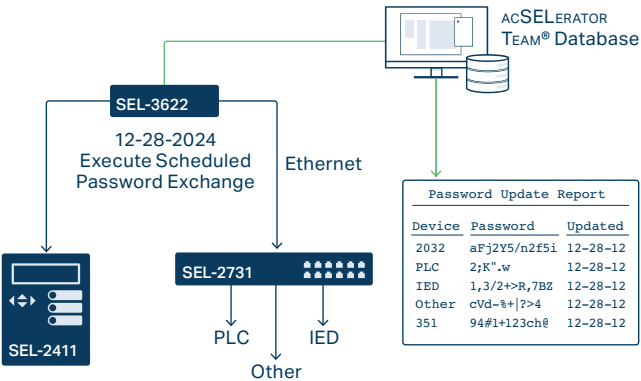
Time Synchronization

Provide time synchronization to all your protected IEDs, data concentrators, and rugged computing devices. Distribute accurate time using both IRIG-B and the Ethernet-based Network Time Protocol (NTP). Should a satellite time source be disrupted temporarily, the SEL-3622 will maintain substation time using its own internal clock.

AcSELerator Team® Database

SEL-3622

12-28-2024
Execute Scheduled
Password Exchange

Ethernet

SEL-2731

SEL-2411

PLC   IED

Other

```
Password Update Report

Device  Password      Updated
2032    aFj2Y5/n2f5i  12-28-12
PLC     2;K".w        12-28-12
IED     1,3/2+>R,7BZ  12-28-12
Other   cVd~%+|?>4    12-28-12
351     94#1+123ch@   12-28-12
```

GPS Clock

SEL-2488

GPS Time Source

IRIG-B

SEL-3622

SEL-651R

NTP

To Control Center

SEL-3530-4

SEL-3622 Specifications

General	
Network Interfaces	**Ports:** 2 rear, 1 front
	Data Rates: 10/100 Mbps
	Front Connector: RJ45 female
	Rear Connectors: RJ45 female or LC fiber (single-mode 100BASE-LX10 or multimode 100BASE-FX)
	VLANs: Up to 4 per physical interface
Serial Ports	Ports: 4 rear
	Type: 2 EIA-232/EIA-485 (software-selectable), 2 EIA-232
	Data Rate: 1200 to 115200 bps
	Connector: DB-9 female (Ports 1—4)
	Protocol Support: Byte- and bit-based serial protocols
Time Synchronization	NTP: Server and client
	IRIG-B Input: Phoenix input, IRIG B000 or B002, even or odd parity
	IRIG-B Output: Serial ports (Pins 4 and 6), IRIG B000 even parity
User Authentication	Local Accounts: 256 maximum local accounts, requires strong passwords (8—128 characters)
	LDAP: v3, TLS-secured
	RADIUS: PAP, EAP-PEAP/MSCHAPv2, EAP-TTLS/PAP
Logging and Alerting	SNMP Traps: v1/v2c/c3
	Syslog: UDP transport
	RADIUS: Accounting packets
Physical Tamper Detection	Input Contact: 1 (pickup/dropout depends on source)
Additional Cybersecurity Controls	Embedded Antivirus: exe-GUARD allowlisting antivirus
	Authorization Levels: Technician and Administrator
	SSH: Server and client
Power Supply Options	12/24 Vdc
	9.8—30.0 Vdc
	<5 Watts
Operating Temperature	−40° to +85°C (−40° to +185°F)

SEL **SCHWEITZER ENGINEERING LABORATORIES**