SEL-3622 Security Gateway

Major Features and Benefits

The SEL-3622 Security Gateway is a compact router, virtual private network (VPN) endpoint, and firewall device that can perform security proxy services for serial and Ethernet-based intelligent electronic devices (IEDs). The small size and low power consumption of the SEL-3622 make it suitable for use in small enclosures such as pole cabinets. Like the SEL-3620, the SEL-3622 helps create an audit trail by using strong, centralized, user-based authentication and authorization to communicate with modern and legacy IEDs. The SEL-3622 secures your control system communication with a stateful deny-by-default firewall, strong cryptographic protocols, and logs for system awareness. The SEL-3622 also manages protected IED passwords, ensuring that passwords are changed regularly and conform to complexity rules for stronger security. The integrated security proxy also provides user-based, single sign-on access to Ethernet and serial connected IEDs.

- **Secure Architecture and Malware Protection.** Maximize reliability with integrated exe-GUARD® whitelist antivirus and other malware protections, eliminating costly patch management and signature updates.
- **Centralized User-Based Access to Protected IEDs.** Provide strong, centralized access control and user accountability to all protected devices with Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS). Simplify compliance with accurate logging.
- **Automated Management of IED Passwords.** Migrate from shared passwords and accounts by using the SEL-3622 as a password manager for protected devices.
- **Security Proxy Services.** Connect securely with identity-based access controls to command line interfaces.
- **Physical Tamper Detection.** Detect and report physical tampering with the built in light sensor, accelerometer, and input contact.
- **Detailed Connection Reports.** Receive detailed connection reports for user activity audits.
- **Secure Ethernet Communication.** Use Internet Protocol Security (IPsec), Media Access Control Security (MACsec), Secure Shell (SSH), and Transport Layer Security (TLS) to provide confidential communication and maintain message integrity among devices.
- **Stateful Deny-by-Default Firewall.** Prevent unauthorized traffic from entering or exiting your private network. Log all successful or blocked connections to the firewall, and receive alerts indicating the presence of unauthorized network communication attempts.

- **Syslog.** Log events for speedy alerts, consistency, compatibility, and centralized collection. For slow communications links, the SEL-3622 can throttle the number of outgoing syslog messages.
- **Integrated Port Switch.** Map one or more of the serial ports to any other serial port, or to Ethernet TCP or UDP connections.
- **Script Engine.** Perform command-driven tasks with a single push of a button, and restrict users to specific scripted tasks.
- **X.509 Certificates.** Ensure strong authentication with third-party validation of incoming connection requests over the IPsec VPN, Active Directory connection, or web management interface.
- **Online Certificate Status Protocol (OCSP).** Use OCSP to verify validity of X.509 certificates.
- **Time Synchronization.** Synchronize events and user activity across your system with IRIG or Network Time Protocol (NTP).
- **Virtual Local Area Networks (VLANs).** Segregate traffic and improve network organization and performance.
- **Ease of Use.** Simplify configuration and maintenance with a secure web interface that allows convenient setup and management.
- **Small Size.** Take advantage of the SEL-3622 gateway's small size, which makes it usable even in small enclosures.
- **Low Power.** Run the SEL-3622 from a battery during power failures; low power consumption extends battery life.
- **Encrypted Terminal Communication.** Securely communicate with IEDs via SSH-encrypted terminal programs.
- **Bit-Based Conversion.** Transform Conitel and other bit-based protocols to Ethernet and reduce reliance on expensive analog circuits.
- **Physical Sensors.** Detect changes in light intensity with an embedded light sensor, motion with an embedded accelerometer, and opening of cabinet doors with a discrete input contact.
- **Reliability.** Rely on the SEL-3622, built for availability, hardened for the substation, and backed by a 10-year warranty.
- **Ethernet Port Bridge.** Support a reliable Ethernet ring topology.
- **Service Port.** Automate base-lining of the device settings with a basic command-line interface.

Functional Overview

The SEL-3622 is a router, VPN endpoint, and firewall device that can provide security proxy services to serial and Ethernet-based IEDs. The SEL-3622 is an access control solution for control systems environments with both Ethernet and serial communication. The SEL-3622 filters all incoming and outgoing traffic with a deny-by-default stateful firewall that only allows authorized traffic. IPsec VPNs protect all site-to-site communication.

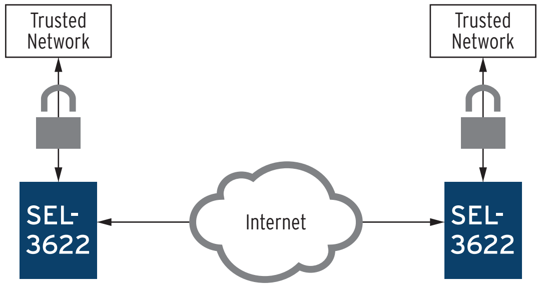


Figure 1 Site-to-Site Virtual Private Network

The authentication proxy technology integrated within the SEL-3622 provides single sign-on engineering access to protected IEDs. The strong authentication in the SEL-3622 includes centralized, user-based credentials and verification of the source of user communication. Thorough logging of all user activities on protected devices provides simple audit reports from which you can know who did what when.

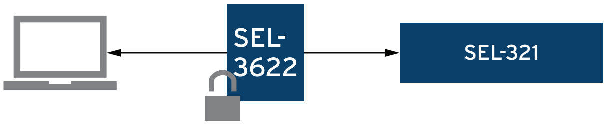


Figure 2 Protected Engineering Access

An integrated, stateful, deny-by-default firewall prevents unauthorized communication from entering or exiting the protected network. The SEL-3622 filters incoming and outgoing TCP, UDP, ICMP, AH, and ESP communication based on a user-configurable set of rules.

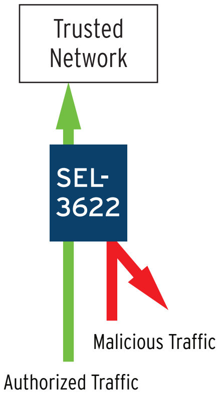


Figure 3 Deny-by-Default Firewall

User-based accounts increase log granularity and make password management easy and effective. The SEL-3622 includes support for centralized authentication and authorization to simplify management of user accounts, passwords, and user privileges for all your protected devices from an active directory server.

The port switch integrated within the SEL-3622 allows users to create mappings for serial-to-serial, serial-to-Ethernet, Ethernet-to-serial, and Ethernet-to-Ethernet communications. By using these mappings, you can use such different modes of communication as one-to-one, one-to-many, and many-to-many.

A Python-based script engine within the SEL-3622 allows users to easily run scripts to perform complicated tasks. These pre-built and customizable scripts can change passwords, navigate complex terminal interface prompts, and perform other tasks that users may need. These scripts can also be an administrative tool for restricting users to a strict set of functional tasks they are authorized to perform.

The SEL-3622 formats, stores, and forwards logs according to the syslog specification to enable quick notification, central collection, and interoperable reporting of security events. IRIG-B and NTP synchronize these events. The SEL-3622 records user activity on IEDs to provide you with auditable tracking of user activity within your system.

Authentication for users of the web management interface, VPN peers, and directory servers relies on X.509 certificates. The Online Certificate Status Protocol (OCSP) verifies the legitimacy of any certificates the SEL-3622 receives.

The SEL-3622 streamlines user-configurable options and uses a Hypertext Transfer Protocol Secure (HTTPS) web interface for a simplified user experience. ACSELERATOR QuickSet® SEL-5030 Software with connection directory software provides configuration of the proxy services. A command line interface on the integrated SSH server provides access to protected IEDs.

The SEL-3622 is built for installations that require high levels of availability. The device contains no moving parts, operates over a wide temperature range from –40°C to +85°C, and uses flash-based data storage for maximum durability.

The SEL-3622 secures traffic by using MACsec. MACsec is a non-routable "hop-by-hop" cryptographic protocol that protects Ethernet frames starting at the data-link layer (OSI Layer 2). The MACsec protocol provides confidentiality, integrity, authenticity, and replay prevention to communications. Automated key management is provided by the MACsec Key Agreement (MKA) protocol. The goal of the MKA protocol is to facilitate and automate the commissioning, management, and scalability of MACsec on a LAN.

Applications

The SEL-3622 is ideally suited for many access point applications: routing, message encryption, packet authentication, and user authentication. The authorization and serial capabilities of the SEL-3622 provide a strong solution for user-based access to legacy IEDs that have shared user accounts.

Secure Communication Over Untrusted Networks

The SEL-3622 secures all communication by establishing IPsec VPN tunnels with other SEL-3620 gateways and IPsec-enabled devices. It can also be used to secure local communications with MACsec.

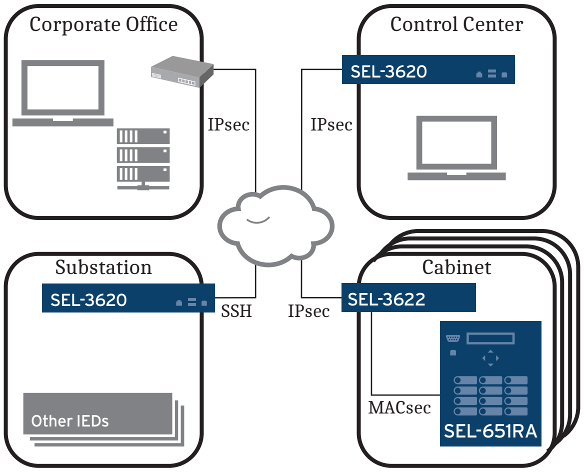


Figure 4 SEL-3622 Encrypts Communication

Routing and Masquerading

The SEL-3622 forwards communication among separate Ethernet networks. Any device that has access to the SEL-3622 can use it to forward Ethernet packets to a destination on a different network.

The SEL-3622 supports Network Address Translation (NAT) for a wide variety of dynamic network applications. Port forwarding enables the use of similar remote address space without re-architecting IP subnets, and outbound NAT supports Internet access for those applications that require it.

Point-to-Point Serial Over Ethernet Network

Figure 5 shows the SEL-3622 in a point-to-point application in which bit- and byte-based serial devices can communicate with each other across an Ethernet network. The SEL-3622 supports IPsec and SSH for encrypted and authenticated communication. This provides an easy transition from existing costly analog serial lines to Ethernet transport networks without having to upgrade remote terminal units (RTU) or communication front ends (CFE).

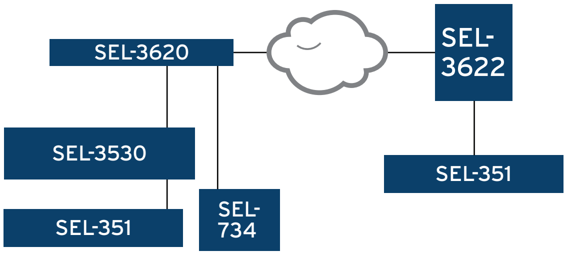


Figure 5 SEL-3622 Protects Serial Over Ethernet

User-Based Access to IEDs

The authentication proxy feature in the SEL-3622 provides user-based access to serial and Ethernet devices within the secured network. The SEL-3622 records and logs all user activity, to provide an audit trail and user accountability.

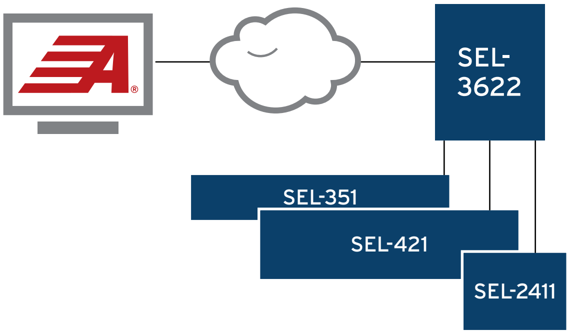


Figure 6 SEL-3622 Authenticates Users

Ethernet-to-Serial Conversions

Gain Ethernet-based access to your serial devices through the SEL-3622. The SEL-3622 performs both bit- and byte-based serial-to-Ethernet media conversions for Telnet, SSH, Raw TCP, and UDP protocols.

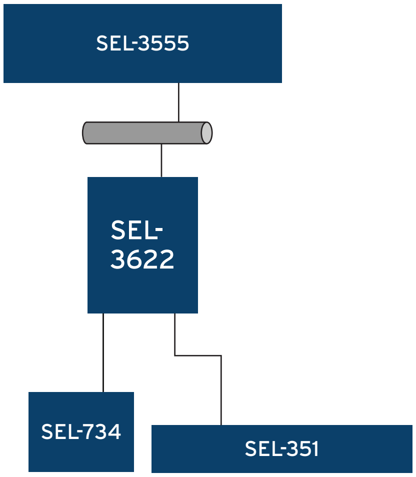
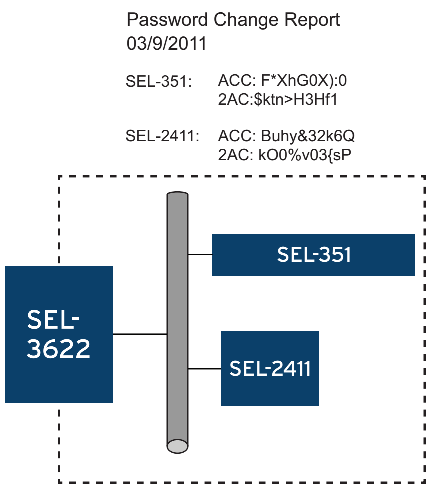


Figure 7 SEL-3622 Converts Serial to Ethernet

Password Management

The SEL-3622 is uniquely designed to manage the passwords of all your protected IEDs. The single sign-on capabilities of the authentication proxy require that the SEL-3622 be aware of the passwords of all protected IEDs. The combination of the script engine with this password knowledge gives the SEL-3622 the ability to manage your passwords, enforce strong passwords, and provide audit reports of password changes.


Password Change Report
03/9/2011

SEL-351: ACC: F*XhG0X):0
2AC:$ktn>H3Hf1

SEL-2411: ACC: Buhy&32k6Q
2AC: kO0%v03{sP

Figure 8 SEL-3622 Manages Passwords

Physical Tamper Detection

Detect and report physical tampering or intrusions to the SEL-3622 installation with the built-in accelerometer, light sensor, and input contact. The accelerometer in the SEL-3622 can detect and alert on both impacts and tilt events to the SEL-3622 or its enclosure. The light sensor detects changes in ambient light levels; useful for reporting enclosure door open or close events. The input contact can also be wired to a door contact or motion detector as an alternate method of reporting intrusions.

Time Distribution

Synchronize all your devices with the SEL-3622, regardless of whether these devices understand NTP or IRIG. The SEL-3622 synchronizes to and sources both IRIG-B and NTP.

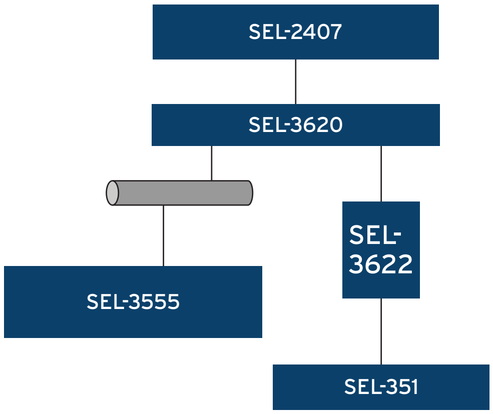


Figure 9 SEL-3622 Distributes Time

Functional Description

Cryptographic Message Protection

IPsec

IPsec VPN initiation requires that three tasks be performed: the two peers must authenticate each other, the Internet Key Exchange (IKE) security associations (SAs) must be established, and the IPsec SAs must be established. Upon establishment of the IPsec SAs, the SEL-3622 transmits all messages that route through this “tunnel” within an Encapsulating Security Payload (ESP). The SEL-3622 performs all of these steps when it connects to any peer IPsec-enabled device.

SAs are shared pieces of information that we can use to secure communications channels. An SA includes the encryption and authentication algorithms the channel uses, along with their respective keys. An IKE SA defines the secure channel on which IPsec SA negotiation takes place. An IPsec SA defines the communications parameters that will be in use for communication across a VPN. The SEL-3622 contains preconfigured settings in “Profiles” to simplify connecting to non-SEL devices.

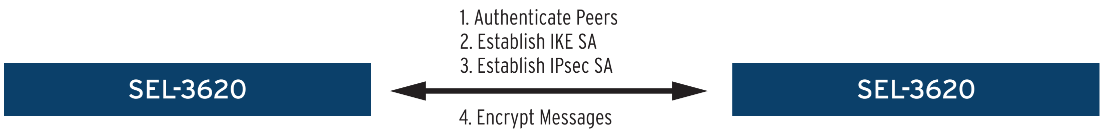


Figure 10 VPN Establishment

Encryption ensures that communication is confidential and only readable by authorized parties. The SEL-3622 uses the IPsec ESP to protect the entire original packet, including both the header and the payload. This prevents information leakage about the structure of your protected networks. The SEL-3622 supports AES and 3DES encryption algorithms.

MACsec

MACsec provides industry-standard security through the use of secured point-to-point Ethernet LAN links. The point-to-point links are secured after matching security keys are exchanged and verified between the interfaces at each end of the point-to-point Ethernet link. Once MACsec is enabled on a point-to-point Ethernet link, all traffic traversing the link is MACsec-secured through the use of data integrity checks and, if configured, encryption. Encryption ensures that communications are confidential and only readable by authorized parties. The SEL-3622 uses MACsec Security Protocols to protect the communication. This prevents the possibility of information leakage.

The SEL-3622 performs all these steps when it connects to any peer MACsec-enabled device. The device will participate as an MKA key server only, not as a client. MACsec is configured in connectivity associations. Key management is automated for simplicity with MACsec and MKA.

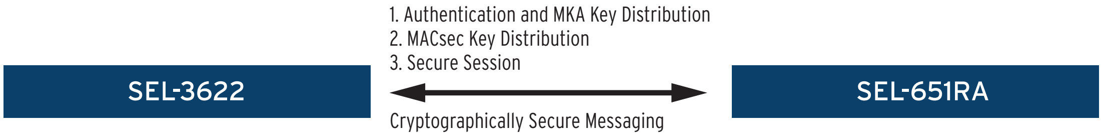

1. Authentication and MKA Key Distribution
2. MACsec Key Distribution
3. Secure Session
SEL-3622
SEL-651RA
Cryptographically Secure Messaging

Figure 11 Layer Two Tunnel Establishment

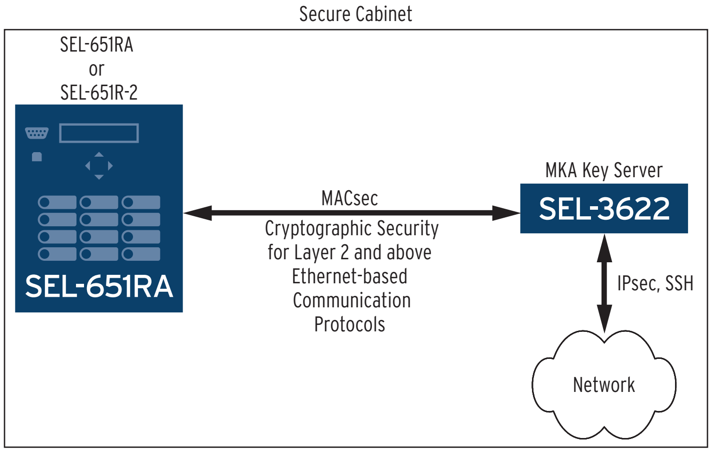


Figure 12 Secure Cabinet

Device Authentication

The SEL-3622 can use either X.509 certificates or preshared keys for authentication of another party over a network. The X.509 certificate confirms that the party at the opposite end of the tunnel is an entity with whom the SEL-3622 has approval to communicate. The SEL-3622 accepts both self-signed X.509 certificates and X.509 certificates that have been signed by a Certificate Authority (CA).

The SEL-3622 uses Online Certificate Status Protocol (OCSP) to check the status of X.509 certificates. When the SEL-3622 receives a connection request along with a certificate signed by a CA, it will poll an OCSP server to verify that the certificate is good. There are three possible responses the OCSP server can supply: good, revoked, and unknown. If the SEL-3622 receives a response other than good, it will deny the connection request.

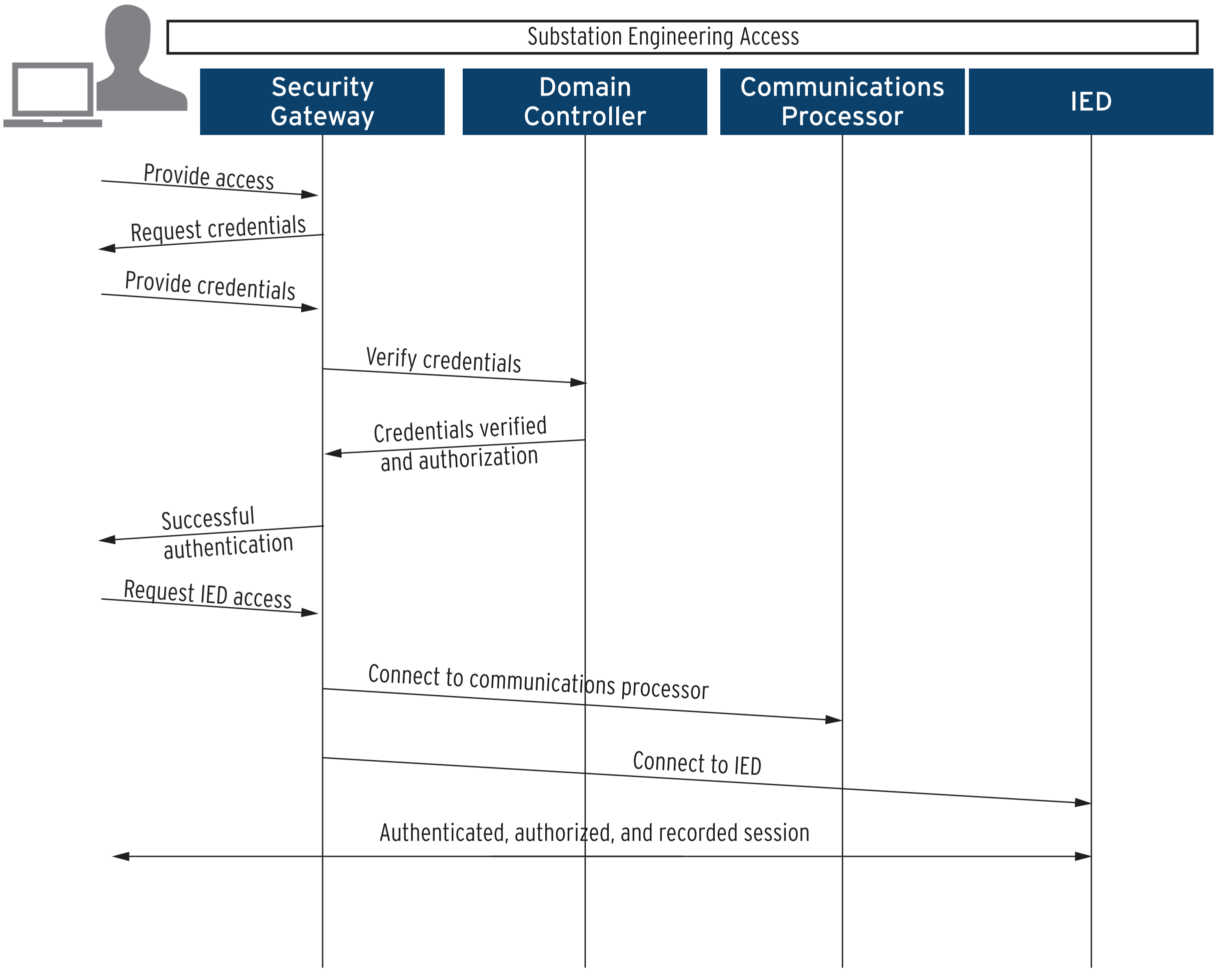

Substation Engineering Access
Security Gateway
Domain Controller
Communications Processor
IED
Provide access
Request credentials
Provide credentials
Verify credentials
Credentials verified and authorization
Successful authentication
Request IED access
Connect to communications processor
Connect to IED
Authenticated, authorized, and recorded session

Figure 13 Central User Authentication

Syslog

The SEL-3622 uses the syslog format to log events. These logs contain several fields that indicate event severity, event origin, event type, and details regarding the cause of the event. Additionally, the event message contains such event tracking information as the entity that triggered the event and the time and date of the event. The SEL-3622 maintains an internal record of as many as 60,000 event logs in nonvolatile memory, and it generates, stores, and forwards syslog messages to multiple destinations.

SNMP

Simple Network Management Protocol (SNMP) support on the SEL-3622 allows administrators to query some state information from the device, as well as to receive notifications (traps) for events that indicate a device integrity fault, such as Mandatory Access Control audit messages, and whitelist integrity failures. The Management Information Base (MIB) provides information about data and traps available via SNMP. The MIB can be downloaded as a zip file from the SEL-3622 from the SNMP Settings page on the web management interface.

Centralized, User-Based Access Control

The security proxy services in the SEL-3622 provide user-based access to protected serial and Ethernet IEDs. *Figure 13* illustrates this process. A user needing to access a protected IED will first access the SEL-3622. The SEL-3622 will then prompt for the username and password. The SEL-3622 will verify the provided credentials with a centralized server and obtain the user's permissions. These permissions then determine which devices and access levels the user has authorization to access. The SEL-3622 connects to the IED that the user wants to access, logs on, and then adds the user to the session, which allows communication between the user and the IED.

Maintaining logs of user activity is very important for auditing purposes. The SEL-3622 monitors all user activity and logs each session to a locally stored file. At the same time, the SEL-3622 generates syslog messages, indicating the start of a session and the end of a session, as an alert that activity has taken place. Users with appropriate privileges can export the user log files for later examination as necessary. Alternately, if the user needs direct relay access, such as for calibration testing purposes, the user can checkout the device. Device checkout resets the device access level passwords, which the user has authorization to access, to their initial values for a preconfigured amount of time.

Multiple Access Methods

Users have multiple methods of accessing IEDs to provide flexibility for various types of software. SSH and Telnet provide a command line interface to protected devices through the SEL-3622. You can also map specific TCP and UDP ports to physical serial ports.

Password Management

The SEL-3622 manages the passwords for all managed devices. It maintains an internal list of all the managed devices, their current states, their initial passwords, their currently used passwords, and their proposed passwords. Password change cycles are broken into three steps:

Step 1. Password generation creates a new list of proposed passwords for all selected managed devices.

Step 2. Report generation and download creates and stores a list of all the currently used and proposed passwords for all managed devices.

Step 3. Password application changes the passwords of all managed device accounts/access levels which have proposed passwords.

The web interface provides a manual method to perform these tasks as needed. The master port self-controller provides a method to easily script these steps for automated systems, such as TEAM Security. The flexibility of the web interface provides a means to enable or disable managed devices so they are not included in bulk operations, as well as the ability to select which devices to generate passwords for. Finally, the web interface provides the ability to set persistent and shared passwords that are never changed as part of a bulk operation.

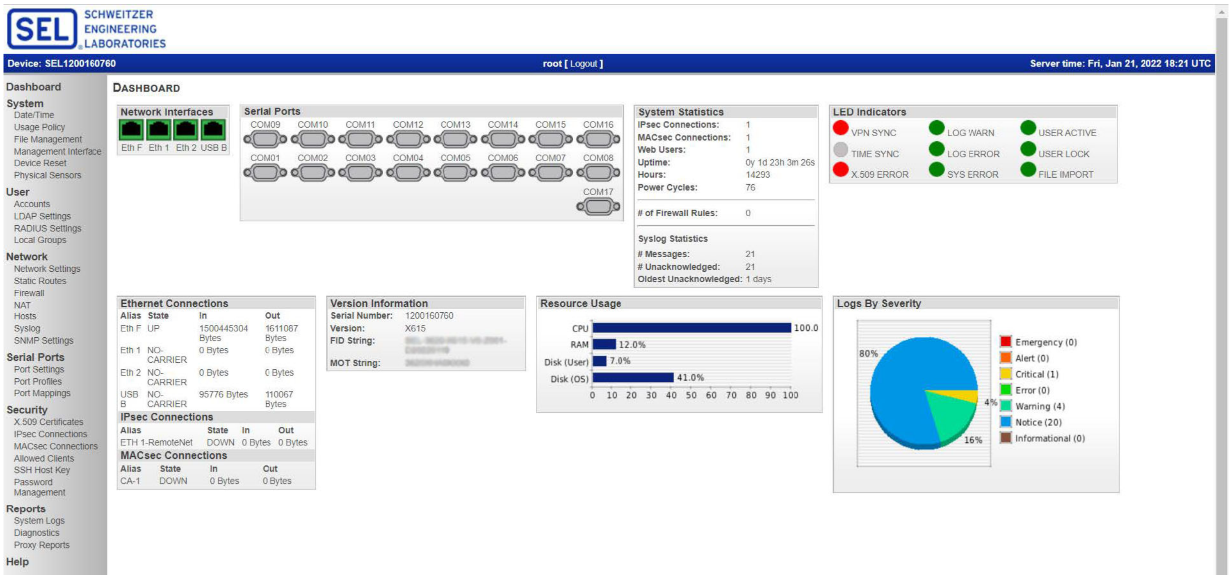
Firewall

To protect your private network from malicious traffic, the stateful firewall in the SEL-3622 denies all traffic by default. Explicitly identifying traffic that the SEL-3622 permits makes it far less likely that the SEL-3622 will overlook specific types of traffic.

Secure Management

Configuration of the SEL-3622 occurs through a secure web management interface that uses HTTPS incorporating transport layer security (TLS). Mutual authentication takes place before a secure web management session opens. The device uses an X.509 server-side certificate to authenticate to the user, and the user uses a username and password to authenticate to the device. The SEL-3622 then restricts users to actions for which they have authorization through their account assignments. There are two roles: administrator and technician. The technician can perform any task on the SEL-3622 except create or edit user accounts, modify date/time settings, or reset, halt, or restart the device. Administrators can perform any action on the SEL-3622, including creating and editing all accounts on the box.

The web management interface provides simple-to-use graphic configuration pages that display the gateway configuration through network diagrams. You can use this to confirm that all configurations are as you intended. The web interface supplies a single place from which you can retrieve all communications channel information and network diagrams associated with the SEL-3622. The device also features a basic command-line interface service port that allows for the automation of configuration base-lining. The service port is read-only and requires administrative credentials to access.



Device: SEL1200160760 root [Logout] Server time: Fri, Jan 21, 2022 18:21 UTC

DASHBOARD

Network Interfaces

Serial Ports

System Statistics

IPsec Connections:	1
MACsec Connections:	1
Web Users:	1
Uptime:	0y 1d 23h 3m 26s
Hours:	14293
Power Cycles:	76
# of Firewall Rules:	0

Syslog Statistics

# Messages:	21
# Unacknowledged:	21
Oldest Unacknowledged:	1 days

LED Indicators

●	VPN SYNC	●	LOG WARN	●	USER ACTIVE
○	TIME SYNC	●	LOG ERROR	●	USER LOCK
●	X.509 ERROR	●	SYS ERROR	●	FILE IMPORT

Ethernet Connections

Alias	State	In	Out
Eth F	UP	1500445304 Bytes	1611087 Bytes
Eth 1	NO-CARRIER	0 Bytes	0 Bytes
Eth 2	NO-CARRIER	0 Bytes	0 Bytes
USB B	NO-CARRIER	95776 Bytes	110067 Bytes

IPsec Connections

Alias	State	In	Out
ETH 1-RemoteNet	DOWN	0 Bytes	0 Bytes

MACsec Connections

Alias	State	In	Out
CA-1	DOWN	0 Bytes	0 Bytes

Version Information

Serial Number:	1200160760
Version:	X615
FID String:	[redacted]
MOT String:	[redacted]

Resource Usage

Logs By Severity

Figure 14 Web Management Dashboard

Mechanical Diagrams and Dimensions

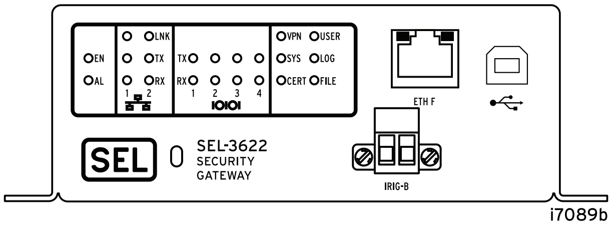


Figure 15 Front-Panel Diagram

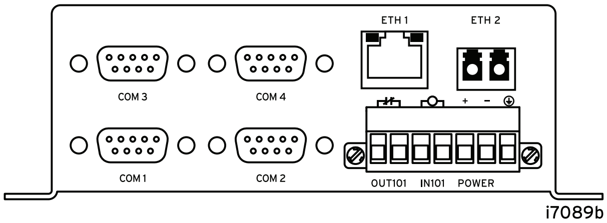


Figure 16 Rear-Panel Diagram (Mixed Technology Ethernet 3622XDE1XXXX Shown)

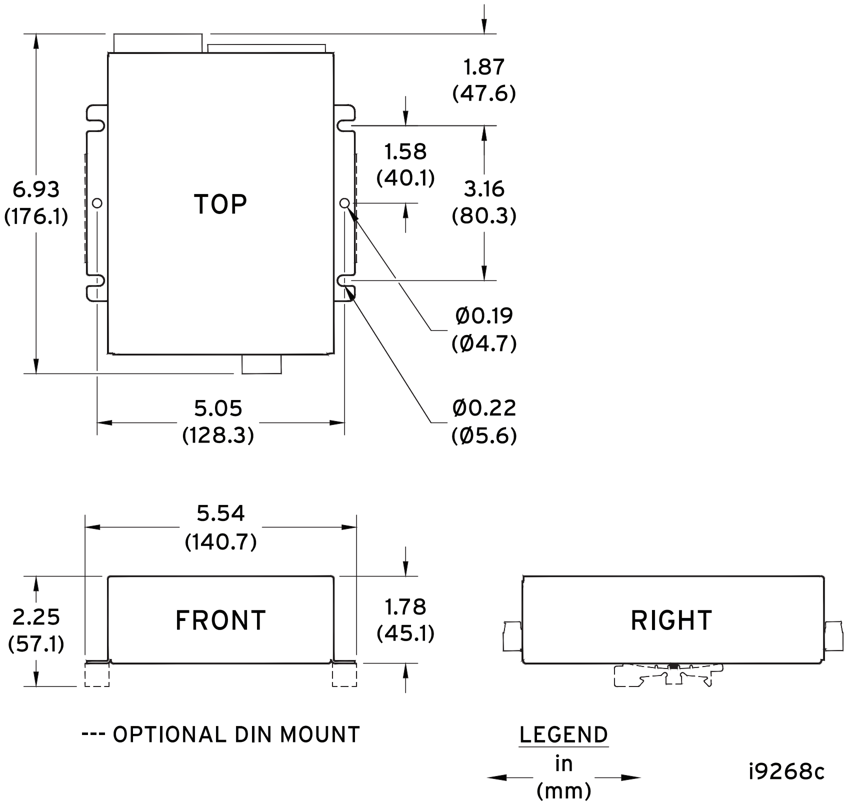


Figure 17 SEL-3622 Dimensions

For IEC 60255-27 compliant applications, the following applies:

The top surfaces of barriers that are accessible in normal use meet at least the requirements of the protective type IP4X. The top has sufficient mechanical strength, stability, and durability to maintain the specified degree of protection and is firmly secured in place in such a way that it can only be removed by the use of a tool. If the unit is mounted in an orientation such that a surface with connectors can be considered the top surface, and the top surface is accessible in normal use, the unit must be installed in an external enclosure to prevent access in normal use. If the external enclosure has a top surface that is accessible in normal use, the top surface of the external enclosure must meet at least the requirements of the protective type IP4X according to IEC 60529 and have sufficient mechanical strength, stability, and durability to maintain the specified degree of protection and be firmly secured in place in such a way that it can only be removed by the use of a tool.

Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

47 CFR 15B, Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at their own expense.

UL Listed to U.S. and Canadian safety standards (File E220228; NRAQ, NRAQ7)

CE Mark
UKCA Mark
RCM Mark

Networking

Web Management

Protection Protocols:	HTTPS, TLSv1.2, TLSv1.3
Authentication:	X.509 and Username/Password
Encryption Key Strength:	128-bit, 256-bit

Virtual Private Networks

Maximum Throughput:	4 Mbps
Maximum Concurrent Sessions:	4
Protection Protocols:	IPsec
Key Exchange:	IKEv1, IKEv2
Authentication:	Passphrase, X.509, OCSP
Nonaccelerated Encryption Algorithms:	AES, 3DES, Blowfish
Encryption Key Strength:	128-bit, 256-bit, 512-bit

Routing Functions

Static Routing

Network Address Translation: Port Forwarding (DNAT) as many as 200 user-specified rules

Network Address Translation: Outbound NAT (SNAT)

Ethernet Protocols

Address Resolution Protocol (ARP)

Dynamic Host Configuration Protocol (DHCP) Client

Dynamic Host Configuration Protocol (DHCP) Server (USB-B Only)

Encapsulating Security Payload (ESP)

File Transfer Protocol (FTP)

Hypertext Transfer Protocol Secure (HTTPS)

Internet Control Message Protocol (ICMP)

Internet Key Exchange (IKEv1/v2)

Internet Protocol Security (IPsec) Protocol Suite

Internet Secure Association and Key Management Protocol (ISAKMP)

Lightweight Directory Access Protocol (LDAP) Client

MACsec Key Agreement (MKA)

Media Access Control Security (MACsec)

Modbus TCP/IP

Network Time Protocol (NTP) Client/Server

Online Certificate Status Protocol (OCSP)

Remote Authentication Dial-In User Service (RADIUS)

Secure Shell version 2 (SSHv2) Client/Server

Simple Network Management Protocol (SNMP)

Spanning Tree Protocol (STP)

Syslog

Telnet

Transmission Control Protocol (TCP)

Transport Layer Security (TLS)

User Datagram Protocol (UDP)

VLAN

Maximum number of VLANs per physical interface:	4

Security

User-Based Accounts

Maximum Local Accounts:	256
Password Length:	8–128 characters
Password Set:	All printable ASCII characters
User Roles:	Administrative and Technician

Syslog

Storage for 60,000 messages

Forwarding to 3 destinations

Firewall

Implementation:	iptables

As many as 1000 user-specified rules supported

Physical Tamper Sensors

Accelerometer, light sensor, discrete contact input

Proxy Services

Maximum number of simultaneous users:	5
Maximum number of managed devices:	25
Time to generate 175 passwords:	<10 minutes

MACsec

Connectivity Associations:	One per physical Ethernet port
Encryption Key:	GCM-AES-128

General

Operating Temperature Range

–40° to +85°C (–40° to +185°F)
Note: Not applicable to UL applications.

Operating Environment

Pollution Degree:	2
Overvoltage Category:	II
Relative Humidity:	5%–95%, non-condensing
Maximum Altitude:	2000 m
Insulation Class:	Class I equipment

Dimensions

Surface Mount:	140.7 mm W x 45.1 mm H x 176.1 D (5.54" W x 1.78" H x 6.93" D)

Weight

0.54 kg (1.2 lb)

Warranty

10 Years

Processing and Memory

Processor Speed:	333 MHz
Memory:	512 MB DDR2 SDRAM
Storage:	2 GB

System Speeds

Firmware Update Time (Variables):	15 min
Cold Boot-Up Time:	3.5 min

Time-Code Input

IRIG accuracy depends on external GPS source

Input Type:	IRIG-B000 or B002, Even or Odd parity

NTP accuracy depends on network conditions

Demodulated IRIG-B (Front-Panel Connector)

On (1) State:	$V_{ih} \geq 2.2$ V
Off (0) State:	$V_{il} < 0.8$ V
Input Impedance:	1.5 kΩ
Accuracy:	250 ns

Network Time Protocol (Ethernet)

Accuracy:	10 ms (varies)

Time-Code Output

IRIG accuracy depends on source accuracy

NTP accuracy depends on network conditions

Demodulated IRIG-B000 Even Parity (Serial)

On (1) State:	$V_{oh} \geq 2.4$ V
Off (0) State:	$V_{ol} \leq 0.8$ V

Output Drive Levels

Serial Port:	TTL 24 mA 2.4 Vdc 120 Ω

Network Time Protocol (Ethernet)

Accuracy:	250 µs (ideal on LAN)

Communications Ports

Ethernet Ports

Ports:	2 rear 1 front
Data Rate:	10 or 100 Mbps interface, 5 Mbps firewall throughput
Front Connector:	RJ45 Female
Rear Connectors:	RJ45 Female or LC Fiber (single-mode or multimode, 100 Mbps only)
Standard:	IEEE 802.3

Fiber Optic

100BASE-FX Multimode Option (to 2 km)

Maximum TX Power:	–14 dBm
Minimum TX Power:	–19 dBm
RX Sensitivity:	–30 dBm
System Gain:	11 dB
Source:	LED
Wavelength:	1300 nm
Connector Type:	LC (IEC 61754-20)

100BASE-LX10 Single-Mode Option (to 15 km)

Maximum TX Power:	–8 dBm
Minimum TX Power:	–15 dBm
RX Sensitivity:	–25 dBm
System Gain:	10 dB
Source:	Laser
Wavelength:	1300 nm
Connector Type:	LC (IEC 61754-20)

Serial Ports

Type:	2 EIA-232/EIA-485 (software selectable on Ports 1 and 2) 2 EIA-232 (Ports 3 and 4)
Data Rate:	1200 to 115200 bps
Connectors:	DB-9 Female (Ports 1–4)
Serial Protocols Supported:	Bit- and Byte-based

USB Port

1 Device Port:	Type B Supports USB Networking with DHCP server for out-of-band management access (driver downloadable from selinc.com)

Power Supply

Complies with IEC HiPot and Impulse standards, except when connected to substation battery. The auxiliary (power supply) circuit should be connected to a battery (or other external power supply meeting application requirements) that is not used for switching inductive loads.

Input Voltage

Rated Supply Voltage:	12–24 Vdc 24–48 Vdc
Input Voltage Range:	9.8–30 Vdc, polarity dependent 19.2–57.6 Vdc, polarity dependent

Power Consumption

DC:	<5 W copper Ethernet; <7 W fiber

Fuse Rating (Internal)

F1:	
Type:	Time lag T
Current Rating:	3.15 A
Voltage Rating:	250 Vac, 300 Vdc

IEC 60127-2/5:	H = 1500 A at 250 Vac,
	p.f. = 0.7–0.8

UL 248-14:	10 kA at 125 Vac,
	p.f. = 0.7–0.8 / 1500 A at 250 Vac,
	p.f. = 0.7–0.8 / 1500 A at 300 Vdc

Input

Optoisolated Control Input

12 Vdc Option

ON:	9.6–18 Vdc
OFF:	<7.2 Vdc
Current Draw at Nominal DC Voltage:	2–6 mA, Nominal is 12 Vdc

24 Vdc Option

ON:	19.2–28.8 Vdc
OFF:	<11 Vdc
Current Draw at Nominal DC Voltage:	4–7 mA, Nominal is 24 Vdc

Electromechanical Output

Ratings

Normally Open (NO):	10th MOT digit is X
Normally Closed (NC):	10th MOT digit is 1
Mechanical Durability:	10 M no-load operations

DC Output Ratings

Voltage:	250 Vdc
Rated Voltage Range*:	24–250 Vdc
Rated Insulation Voltage:	300 Vdc
Utilization Category:	DC-13
Pilot Duty Ratings[†]:	R300, 250 Vdc
Make (Short Duration Contact Current)*:	30 A @ 250 Vdc
Continuous Carry*:	6 A @ 70°C; 4 A @ 85°C
Thermal*:	50 A for 1 s
Contact Protection:	360 Vdc, 40 J MOV protection across open contacts
Operation Time (Coil Energization to Contact Closure, Resistive Load)*:	Pickup/Dropout Time ≤ 8 ms typical

Breaking Capacity (10,000 Operations)*:

48 V	0.50 A	L/R = 40 ms
125 V	0.30 A	L/R = 40 ms

Cyclic Capacity (2.5 cycles/second)*:

48 V	0.50 A	L/R = 40 ms
125 V	0.30 A	L/R = 40 ms

AC Output Ratings

Rated Operational Voltage:	240 Vac
Rated Voltage*:	110–240 Vac
Rated Insulation Voltage:	300 Vac
Utilization Category:	AC-15 (control of electromechanic loads > 72 VA)
Pilot Duty Ratings[†]:	B300, 240 Vac
Contact Protection:	270 Vac, 40 J
Continuous Carry*:	6 Arms @ 70°C; 4 Arms @ 85°C
Rated Frequency:	50/60 ±5 Hz
Operating Time (Coil Energization to Contact Closure)*:	Pickup/Dropout Time ≤ 8 ms

* Parameters verified by SEL per IEC 60255-1:2009 and IEEE C37.90-2005.

[†] Per UL 508.

Solid-State Output Contact (Units Manufactured Prior to April 2017)

Ratings

100 mA continuous

250 Vdc or 120 Vac Operational Voltage

Maximum On Resistance:	50 Ω
Minimum Off Resistance:	10 MΩ
Insulation:	2500 Vdc
Wiring Size:	14 AWG Max. 26 AWG Min. 0.4 mm Min. Insulation 105°C, 250 V Min.

Product Standards

Communications Equipment in Utility Substations:	IEC 61850-3:2013 IEEE 1613-2009 Severity Level: Class 1
Measuring Relays and Protection Equipment:	IEC 60255-26:2013* IEC 60255-27:2013

* Acceptance Criteria C applied to 0% dc voltage dips for 10 ms. The auxiliary (power supply) circuit is intended to be connected to a battery (or other external power supply meeting application requirements) that is not used for switching inductive loads and will provide the required hold-up time.

Type Tests

Environmental Tests

Enclosure Protection:	IEC 60529:2001 + CRGD:2003 Severity Level: IP30 (excluding the terminal blocks)
Vibration Resistance:	IEEE 1613-2009 IEC 60255-21-1:1988 Severity Level: Endurance Class 2 Response Class 2
Shock Resistance:	IEEE 1613-2009 IEC 60255-21-2:1988 Severity Level: Shock Withstand, Bump Class 1 Shock Response Class 2
Seismic:	IEC 60255-21-3:1993 Severity Level: Quake Response Class 2

Cold, Operational and Storage:	IEC 60068-2-1:2007 Severity Level: –40°C, 16 hours
Dry Heat, Operational and Storage:	IEC 60068-2-2:2007 Severity Level: 85°C, 16 hours
Damp Heat, Cyclic:	IEC 60068-2-30:2005 Severity Level: 25–55°C, 6 cycles, 95% relative humidity
Damp Heat, Steady State:	IEC 60068-2-78:2012 Severity Level: +40°C, 240 hours, 93% relative humidity

Dielectric Strength and Impulse Tests

The following IEC standards only apply if the device is not connected directly to the station battery.

Dielectric (HiPot):	IEC 60255-27:2013 IEEE C37.90-2005 Class B, Section 8: Dielectric Tests Dielectric Strength Section Severity Level: 2500 Vac for one minute on contact inputs, contact outputs 1600 Vdc for one minute on power supply
Impulse:	IEC 60255-27:2013 IEEE C37.90-2005 Class B Severity Level: 0.5 Joule, 2.5 kV

RFI and Interference Tests

EMC Immunity

Electrostatic Discharge Immunity:	IEEE C37.90.3-2001 IEC 61000-4-2:2008 Severity Level: 2, 4, 6, 8 kV contact discharge; 2, 4, 8, 15 kV air discharge
Magnetic Field Immunity:	IEC 61000-4-8:2009 Severity Level: 1000 A/m for 3 seconds, 100 A/m for 1 minute IEC 61000-4-9:2001 Severity Level: 1000 A/m
Power Supply Immunity:	IEC 61000-4-11:2004 IEC 61000-4-17:1999+A1:2001+A2:2008 IEC 61000-4-29:2000
Radiated RF Immunity:	IEC 61000-4-3:2010 Severity Level: 10 V/m, IEEE C37.90.2-2004 Severity Level: 35 V/m
Fast Transient, Burst Immunity:	IEC 61000-4-4:2012 Severity Level: 4 kV @ 5.0 kHz 2 kV @ 5.0 kHz for comm. ports
Surge Withstand Capability Immunity:	IEEE C37.90.1-2002 Severity Level: 2.5 kV oscillatory 4 kV fast transient IEC 61000-4-18:2006 + A1:2010 Severity Level: 2.5 kV common-mode 1.0 kV differential-mode 1 kV common-mode on comm. ports
Surge Immunity:	IEC 61000-4-5:2005 Severity Level: 1 kV line-to-line 2 kV line-to-earth 2 kV comm. ports
Conducted RF Immunity:	IEC 61000-4-6:2008 Severity Level: 10 Vrms
Digital Radio Telephone RF Immunity:	ENV 50204:1995 Severity Level: 10 V/m at 900 MHz and 1.89 GHz

EMC Emissions

Radiated and Conducted Emissions:	CISPR 11:2009+A1:2010 CISPR 22:2008 ANSI C63.4-2014 Class A Canada ICES-001 (A) / NMB-001 (A)

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

PDS3622-01