SEL-5057 Flow Auditor Instruction Manual

Automate Data Collection for NERC CIP-007-6 R1.1 Audit and Document Every Network Host and Conversation

Major Features and Benefits

The SEL-5057 Flow Auditor is an application that operates in combination with your software-defined network (SDN) to provide a safe, nondisruptive audit. It also provides documentation of your network access control by recording the host attributes you have determined to allow, the locations where you have specified hosts can physically connect, and the conversations you have permitted for each host. The Flow Auditor reads OpenFlow configurations from the SEL-5056 Software-Defined Network (SDN) Flow Controller and reports all devices, ports, and services you have allowed.

This application, which automates the collection of SDN data necessary for compliance to NERC CIP-007-6 R1.1, provides the following:

- **Inline Non-Bypassable Restricted Network Access Control Auditing.** Audit and report ports and services.
- **Asset Management.** Automate the discovery and documentation of all authorized devices.
- **Ease of Use.** Simple to use on-screen instructions, quick scalability, and exportable reports.
- **Safe, Disruptionless Auditing.** Provide network access control audits without traffic disruptions, injecting additional packets, or the need to log in to field devices.
- **Cybersecurity.** Establish detailed situational awareness in which you know what devices are on your network and what conversations each device can have. Connect securely to the SEL-5056 through the use of HTTPS.
- **Simple One-Time Licensing.** Obtain perpetual licensing on the purchased version with an end-user license agreement that allows no-cost upgrades for one year.

Functional Overview

The Flow Auditor audits the host-based network access control (NAC). This NAC audit documents both the physical and logical access controls for each host allowed to connect to the SDN and generates the final report internally and provides a comma-separated value (CSV) format for exporting.

Reporting

The Flow Auditor automates the collection of flow tables and uses information from the flow tables to answer three main questions for the network owner.

1. What devices are allowed on my network?
2. Where are these devices allowed to physically connect?
3. What conversations are each device allowed to have?

These reports are device-centered, showing the conversations allowed between the end devices and providing directionality, so you can understand which device initiates conversations. The highest order of attribute is listed so you can associate the conversation with the application or service. For example, the Flow Auditor lists any TCP or UDP ports of which it is aware, allowing the conversation on the TCP port to be associated with the communicating application. An example might be an association of TCP Port 443 with HyperText Transfer Protocol Secure (HTTPS).

The Flow Auditor allows you to enter a justification for each conversation it discovers in the network. This justification is a string that then appears in the final report supporting the justification requirements for NERC CIP-007-6 R1.1. Once you have entered a justification, you can use it on every conversation that displays identical attributes, simplifying data entry.

The report identifies the user who initiated the Flow Audit and exported information and provides a time stamp showing when the audit occurred.

NERC CIP-007-6 R1 Support

The Flow Auditor provides a report that supports NERC CIP-007-6 R1.1 port and services compliance requirements by showing all the devices on the network and all the conversations each device is allowed. SDN is an inline non-bypassable security control that is used to identify and document the ports and services that hosts have open. SDN manages the ports and services allowed on the local area network (LAN), and the Flow Auditor provides reports on these ports and services. The use of SDN for the LAN and the use of the Flow Auditor can therefore eliminate the need for port scanning and field work orders, saving time and cost.

Installation

Download the Flow Auditor application installer from the SEL website. The Flow Auditor supports Windows 10 and Windows Server 2016 and can be installed on any computer that either has SEL-5056 installed or that can network to SEL-5056 Flow Controllers. After downloading the installer from the SEL website, use Administrator privileges and follow the on-screen steps the installer presents to install and run the application.

Software Updates

To upgrade an existing version of the Flow Auditor on your computer, run the same installer that you would run for a new installation. The installer detects the version of the Flow Auditor already installed and prompts you to uninstall the previous version before the installer can continue. You must apply Flow Auditor upgrades in release order without skipping a version in order to maintain all configurations and settings.

Licensing and End-User License Agreement

The Flow Auditor requires a 30-day demonstration license or a perpetual license before it will operate. There are no annual maintenance costs. Once licensed, upgrades to newer versions released within one year are included. You can purchase licenses by contacting SEL sales. Find your sales contact at selinc.com/support.

Creating, Displaying, and Exporting Audit Reports

The Flow Auditor generates audit reports on demand. Audits are performed without disrupting the operational network and without injection of any packets on the network. This is a safe and preferred alternative to network scanning for performing audits to discover and document every device on the network and what ports and services each device is running. The audit pulls the flow tables for each switch in the network from the SEL-5056 and computes what devices can connect to the network, where those devices can connect, and what conversations each of those devices are allowed to have. OT SDN is a deny-by-default, whitelisted, and proactive traffic-engineered solution, so the SDN switches are classified as an inline non-bypassable security control in NERC CIP-007-6 R1.1. You can run audits as often as desired with no impact to the performance of the operational network. The Flow Auditor database stores these reports. You can use the user interface to retrieve and export these reports.

Generating Reports

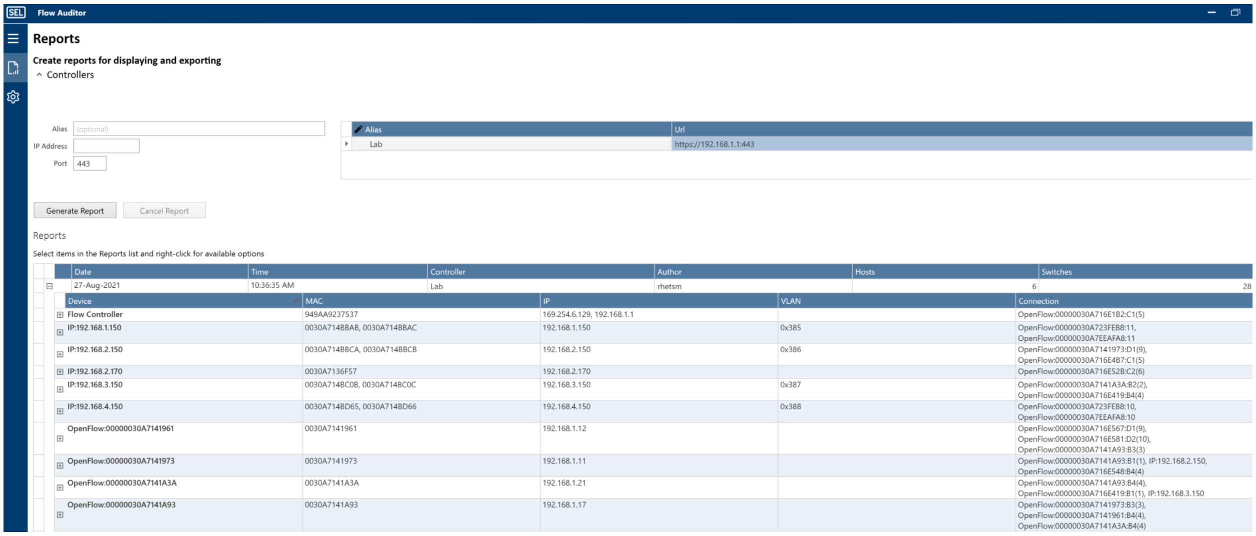
Navigate to the reports page in the Flow Auditor and select the controller you would like to audit. If this is the first time you have audited this controller, type in the optional alias, IP address, and port number the controller user interface is listening on. Then select **Generate Report**. This will bring up a login prompt. Log in with a valid SEL-5056 user account. The status indicators next to the SEL-5056 indicate when the report is complete. Each new report displays in the report list. You can use each column to sort the entire report list, and you can move the columns by dragging and dropping them to establish your preferred order.

Displaying Reports

The generated report displays the report list. Initially in this list each report shows the date and time the report was generated, the name of the SEL-5056 that provided the data from which the report was generated, the Windows username of the user who generated the report, and how many switches and hosts are included in the report. Expand the Device Tier of the report by clicking the left-justified plus sign.

Device Tier

The Device Tier lists all the devices allowed to connect to the network. This list includes all hosts and switches and includes all network segments that the SEL-5056 manages. At this tier, device attributes also display. These include the MAC, IP address, any VLAN tags the device is publishing, and the port on the SDN switch to which the device is connected. *Figure 1* shows all device ports that are connected to the network.



Reports

Create reports for displaying and exporting

Controllers

Alias (optional)

IP Address

Port 443

Alias	Url
Lab	https://192.168.1.1:443

Reports

Select items in the Reports list and right-click for available options

Date	Time	Controller	Author	Hosts	Switches
27-Aug-2021	10:36:35 AM	Lab	rhetsm	6	28

Device	MAC	IP	VLAN	Connection
Flow Controller	949AA9237537	169.254.6.129, 192.168.1.1		OpenFlow:00000030A716E1B2:C1(5)
IP:192.168.1.150	0030A714BBAB, 0030A714BBAC	192.168.1.150	0x385	OpenFlow:00000030A723FEB8:11, OpenFlow:00000030A7EEAFA8:11
IP:192.168.2.150	0030A714BBCA, 0030A714BBCB	192.168.2.150	0x386	OpenFlow:00000030A7141973:D1(9), OpenFlow:00000030A716E4B7:C1(5)
IP:192.168.2.170	0030A7136F57	192.168.2.170		OpenFlow:00000030A716E52B:C2(6)
IP:192.168.3.150	0030A714BC0B, 0030A714BC0C	192.168.3.150	0x387	OpenFlow:00000030A7141A3A:B2(2), OpenFlow:00000030A716E419:B4(4)
IP:192.168.4.150	0030A714BD65, 0030A714BD66	192.168.4.150	0x388	OpenFlow:00000030A723FEB8:10, OpenFlow:00000030A7EEAFA8:10
OpenFlow:00000030A7141961	0030A7141961	192.168.1.12		OpenFlow:00000030A716E567:D1(9), OpenFlow:00000030A716E581:D2(10), OpenFlow:00000030A7141A93:B3(3)
OpenFlow:00000030A7141973	0030A7141973	192.168.1.11		OpenFlow:00000030A7141A93:B1(1), IP:192.168.2.150, OpenFlow:00000030A716E548:B4(4)
OpenFlow:00000030A7141A3A	0030A7141A3A	192.168.1.21		OpenFlow:00000030A7141A93:B4(4), OpenFlow:00000030A716E419:B1(1), IP:192.168.3.150
OpenFlow:00000030A7141A93	0030A7141A93	192.168.1.17		OpenFlow:00000030A7141973:B3(3), OpenFlow:00000030A7141961:B4(4), OpenFlow:00000030A7141A3A:B4(4)

Figure 1 Reports Page Device Tier

You can drag and drop each column in Device Tier into your preferred order and sort each column by clicking the column header. Clicking the plus sign on any listed device expands the Conversation Tier of the report for that device.

Conversation Tier

The Conversation Tier shows all conversations each device is permitted to have. For layer two conversations, the EtherType displays in hexadecimal. For IP conversations, IP displays. For all TCP and UDP conversations, the port number displays if the port is used for flow management. Otherwise, only TCP and UDP display.

When IP displays as a conversation, all IP-based communications are allowed between the device and the sources and destinations listed.

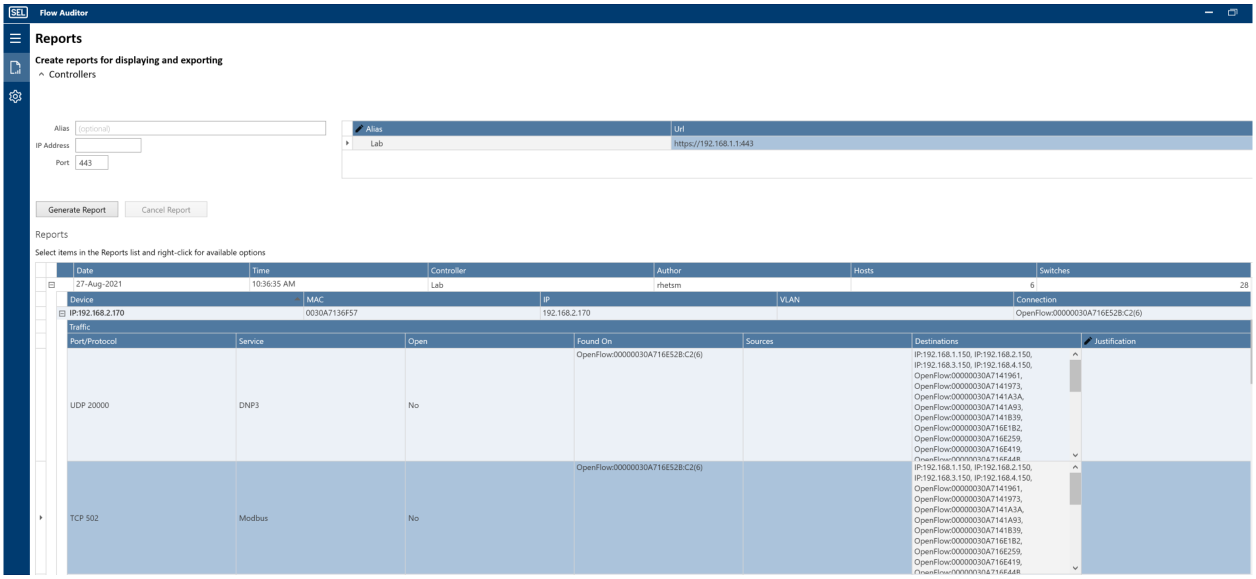
When TCP or UDP is listed, all ports are allowed between this device and the listed sources and destinations.

When there is a TCP or UDP with a port number, only that specific protocol is allowed between this device and the listed sources and destinations. These conversations show directionality.

The devices listed as sources for each conversation are the remote devices allowed to initiate a conversation with the listed device. This means that the device you expanded has a listening port open and that the network allows the source to have this conversation with this device.

The devices listed as destinations for each conversation are the remote devices with which the device in this report can initiate this type of conversation.

The screen capture in *Figure 2* shows that Feeder B has TCP Port 502 open and listening for the incoming connection from the RTAC.



Reports

Create reports for displaying and exporting

^ Controllers

Alias: (optional)

IP Address:

Port: 443

Alias	Url
Lab	https://192.168.1.1:443

Reports

Select items in the Reports list and right-click for available options

Date	Time	Controller	Author	Hosts	Switches
27-Aug-2021	10:36:35 AM	Lab	rhetsm	6	28

Device	MAC	IP	VLAN	Connection
IP:192.168.2.170	0030A7136F57	192.168.2.170		OpenFlow:00000030A716E52B:C2(6)

Traffic

Port/Protocol	Service	Open	Found On	Sources	Destinations	Justification
UDP 20000	DNP3	No	OpenFlow:00000030A716E52B:C2(6)		IP:192.168.1.150, IP:192.168.2.150, IP:192.168.3.150, IP:192.168.4.150, OpenFlow:00000030A7141961, OpenFlow:00000030A7141973, OpenFlow:00000030A7141A3A, OpenFlow:00000030A7141A93, OpenFlow:00000030A7141B39, OpenFlow:00000030A716E1B2, OpenFlow:00000030A716E259, OpenFlow:00000030A716E419, OpenFlow:00000030A716E44B	
TCP 502	Modbus	No	OpenFlow:00000030A716E52B:C2(6)		IP:192.168.1.150, IP:192.168.2.150, IP:192.168.3.150, IP:192.168.4.150, OpenFlow:00000030A7141961, OpenFlow:00000030A7141973, OpenFlow:00000030A7141A3A, OpenFlow:00000030A7141A93, OpenFlow:00000030A7141B39, OpenFlow:00000030A716E1B2, OpenFlow:00000030A716E259, OpenFlow:00000030A716E419, OpenFlow:00000030A716E44B	

Figure 2 Reports Page Conversation Tier

When you see a device listed in both source and destination for the same conversation, either side is allowed to initiate the listed conversation. You can drag and drop each column in Conversation Tier into your preferred order and sort each column by clicking the column header. You can enter justification for each conversation by double-clicking the row for the conversation. There are two options for applying justification:

1. Update this row—this applies the justification to that row only.
2. Update same traffic type in this report—this updates all conversations with the same protocol and service in the same report but will not update any other report.

Each conversation in the report is as specific as the OpenFlow match criteria used in the flows. When exact match criteria are used at multiple layers, the conversation audit becomes more specific. When more open flows are used, the conversation audit becomes less specific. The conversation audit cannot include TCP or UDP ports if the flows do not include them, and the same is true with the input ports on the switch; input ports must be used in the flow before they will be part of the conversation audit.

Audits With Traditional Switches

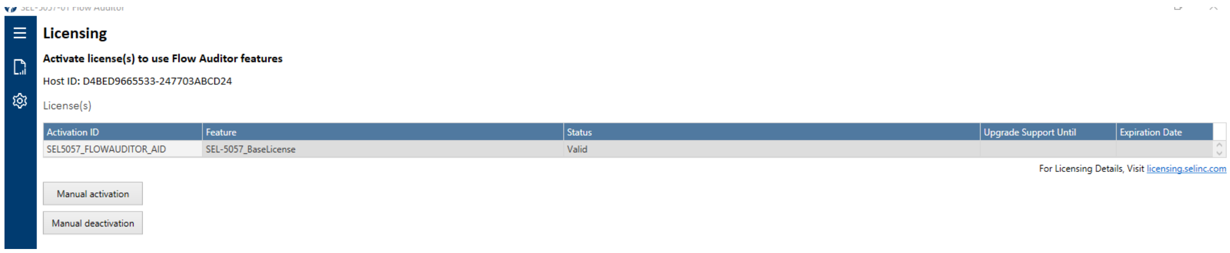
The Flow Auditor provides an audit to the best of its ability in hybrid networks where there are SDN switches and spanning tree switches. When the Flow Auditor does not know the exact destination because there is no specific destination address, it adds an indicator (*) to the report. For example, the Flow Auditor places an * in the report when a multicast packet is passed to the spanning tree switch and the Flow Auditor no longer has the ability to determine where that multicast packet is delivered.

Exporting Reports

Select the report(s) in the list you want to export by clicking anywhere in the row. The Flow Auditor supports selection of multiple items. Once you have selected the desired report(s) you want, right-click them and select **Export Selected Reports**. Navigate to the location where you want to save the report, name the report, and select **Save**.

Licensing

The licensing page supports the upload of a new license.



Licensing

Activate license(s) to use Flow Auditor features

Host ID: D4BED9665533-247703ABCD24

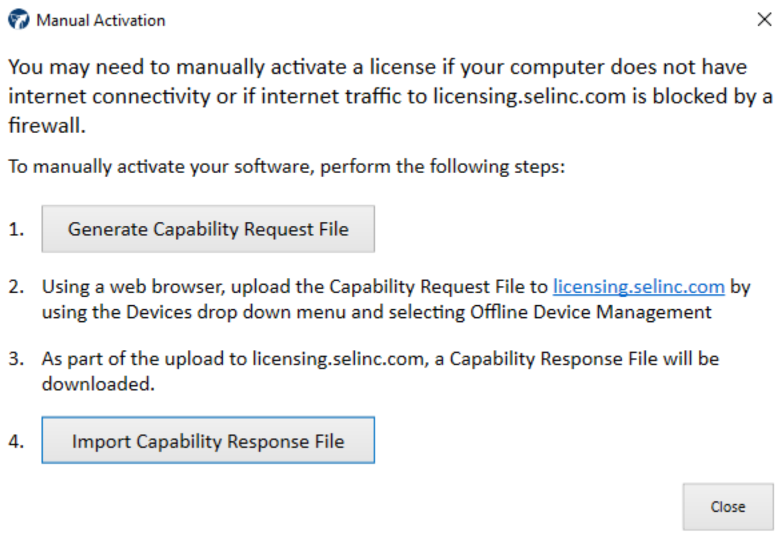
License(s)

Activation ID	Feature	Status	Upgrade Support Until	Expiration Date
SEL5057_FLOWAUDITOR_AID	SEL-5057_BaseLicense	Valid		

For Licensing Details, Visit licensing.selinc.com

Figure 3 Licensing Page

Click **manual activation** and follow the on-screen instructions.



Manual Activation

You may need to manually activate a license if your computer does not have internet connectivity or if internet traffic to licensing.selinc.com is blocked by a firewall.

To manually activate your software, perform the following steps:

1. Generate Capability Request File
2. Using a web browser, upload the Capability Request File to licensing.selinc.com by using the Devices drop down menu and selecting Offline Device Management
3. As part of the upload to licensing.selinc.com, a Capability Response File will be downloaded.
4. Import Capability Response File

Figure 4 License Activation

Information Page

Click the “I” symbol in the bottom left corner of the application to navigate to the information page. This page displays the Flow Auditor version information and any required credits.

Copyrighted Software

The Flow Auditor includes copyrighted software, licensed under the following user agreement.

Security

Overview

The version information for the Flow Auditor is found under the information icon in the lower left corner of the user interface.

Security Controls

Available security controls in the Flow Auditor are as follows:

- **Open Ports.** The Flow Auditor only has one port open by default on Port 443. The port used by the Flow Auditor is changed using the Binding Settings.
- **Default Accounts.** None.
- **User Accounts.** The Flow Auditor has no user accounts in the application but rather uses the access control permissions supervised by the Windows operating system. All logs associated with user actions will use the Windows username.

- **User Roles.** The Flow Auditor has only one role. The Windows operating system manages this role by which users can access the computer on which the local Flow Auditor is operating and access the Flow Auditor. The Flow Auditor only reads data from the operational SEL-5056 and is unable to make changes.
- **Logging.** All logs are recorded to the Windows Event Viewer, which tags actions by the user with the Windows username of that user.
- **Updates and Maintenance.** The Flow Auditor can be updated by running the installer. This removes older versions and updates the Flow Auditor to the newer version. All versions of the Flow Auditor are digitally signed by SEL.
- **Recommendations.** Use hard drive encryption.

Cybersecurity

The Flow Auditor has no login for the application itself. Access to the application is managed by access to the computer on which the application is operating. The Flow Auditor communicates to the registered SEL-5056 through HTTPS and mutually authenticates the Flow Auditor to the SEL-5056 through X.509 certificates exchanged during the commissioning and registration process. The Flow Auditor only reads data from the SEL-5056 and supports no write actions.

Security Support

Contact SEL security with any additional questions or concerns at:

security@selinc.com
Tel: +1.509.332.1890

Specifications

Operating System Support

Windows Server 2016 Standard
Windows 10

General

Protocols

Transport Layer Security (TLS)
Windows group policy manages the cipher negotiation policies

Security

X.509 certificate
User-based accounts

Disk Space

1 G or larger

Third-Party Software

Microsoft .NET Framework 4.7.2

Software Versions

Determining the Software Version

The software version number displays on the bottom left of each webpage after the user has successfully logged into the Flow Auditor.

Revision History

Table 1 lists the lists the Flow Auditor software versions, revision descriptions, and corresponding instruction manual date codes.

Table 1 SEL-5057 Flow Auditor Software Revision History

Software Version Number	Summary of Revisions	Manual Date Code
2.0.1.1	➤ Added support for the SEL-2741 Ethernet Switch. ➤ Enhanced report generation to only include adopted objects.	20230731
2.0.1.0	➤ Updated 3rd party library for performance enhancements.	20230104
2.0.0.0	➤ Added support for Flow Controller operating on Blueframe. ➤ Added the ability to connect to SEL-5056 Flow Controller through the use of a username and password. ➤ Removed the requirement to register the Flow Auditor with each Flow Controller. ➤ Addressed an issue that in previous releases did not render results from OpenFlow instructions that output to ALL switch ports correctly.	20210924
1.1.0.0	➤ Improved audit support for layer-two-only hosts. ➤ Improved support for audits with traditional switches in the network. ➤ Filtered audits for TCP Port 0.	20200930
1.0.0.0	➤ Initial version.	20200731

Instruction Manual Versions

The date code at the bottom of each page of this manual reflects the creation or revision date.

Table 2 lists the instruction manual versions and revision descriptions. The most recent instruction manual version is listed first.

Table 2 Instruction Manual Revision History

Date Code	Summary of Revisions
20230731	➤ Updated for version 2.0.1.1.
20230104	➤ Updated for version 2.0.1.0.
20210924	➤ Updated *Major Features and Benefits*. ➤ Updated *Installation*. ➤ Updated *Creating, Displaying, and Exporting Audit Reports*. ➤ Updated for version 2.0.0.0.
20200930	➤ Added a new *Software Updates* section under *Installation*. ➤ Added a new *Audits With Traditional Switches* section under *Creating, Displaying, and Exporting Audit Reports*. ➤ Updated for version 1.1.0.0.
20200911	➤ Updated *Flow Auditor and SEL-5056 Steps* under *Installation*. ➤ Updated *Specifications*.
20200731	➤ Initial version.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

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 selinc.com or contact your customer service representative.

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

ISO 9001 CERTIFIED

WORLDWIDE 10 years WARRANTY