SEL-FLT and SEL-FLR

Fault and Load Transmitter and Receiver System

Instruction Manual

20230106

SEL SCHWEITZER ENGINEERING LABORATORIES

PMFLT-FLR-01

Table of Contents

Section 6: Diagnostics

Section 7: SEL-FLT Features

Section 8: SEL-FLT Event Detection

Section 9: Maintenance, Testing, and Troubleshooting

Appendix A: Firmware and Manual Versions

Appendix B: DNP3 Profile and Data Map

Appendix C: Syslog

Appendix D: Link Budget Analysis

Appendix E: X.509

This page intentionally left blank

List of Tables

This page intentionally left blank

List of Figures

This page intentionally left blank

Preface

Overview

The SEL-FLR and SEL-FLT make up a system for monitoring load and detecting faults on distribution circuits for electric utilities and industrial applications. The SEL-FLT Fault and Load Transmitters are line-mounted sensors that send information to an SEL-FLR Fault and Load Receiver acting as a network concentration point.

This manual describes common aspects of fault and load monitoring applications, including information on installing, configuring, testing, and operating the SEL-FLT/SEL-FLR system.

An overview of each manual section and topics follows:

Preface. Provides the manual overview, as well as safety and general information about the product.

Section 1: Introduction and Specifications. Introduces SEL-FLT and SEL-FLR features, summarizes functions, and lists specifications, type tests, and ratings.

Section 2: Installation. Provides product dimensions, installation instructions, and information about SEL-FLT activation and SEL-FLR grounding, antennas, and surge protection. Explains the basic steps to set up, configure, and commission the SEL-FLT and SEL-FLR system.

Section 3: Applications. Describes common scenarios on the distribution system that benefit from applying the SEL-FLT and SEL-FLR system.

Section 4: SEL-FLR Configuration. Provides information on the wireless network behavior and protocol. Includes information about the radio network, SEL-FLT whitelist and sensor management, Ethernet network interfaces, DNP3 communication, and SEL-FLT parameters and settings.

Section 5: System. Describes the SEL-FLR settings interface for date and time, web server settings, usage policy, contact information, user accounts, file management, X.509 certification management, and device reset.

Section 6: Diagnostics. Describes alarm contact connections and operation, local and remote Syslog operation, severity thresholds, event acknowledgment, and report fields and filters.

Section 7: SEL-FLT Features. Provides an overview of basic features and functionality of the SEL-FLT, including the local display, device arming, load monitoring, and message types and data.

Section 8: SEL-FLT Event Detection. Explains the system conditions required for the SEL-FLT to arm, as well as outage detection and fault detection behavior.

Section 9: Maintenance, Testing, and Troubleshooting. Describes techniques for testing, troubleshooting, and maintaining the SEL-FLT and SEL-FLR.

Appendix A: Firmware and Manual Versions. Lists the current firmware versions and details differences between the current and previous versions.

Appendix B: DNP3 Profile and Data Map. Lists the DNP3 profile and data map for the SEL-FLT and SEL-FLR.

Appendix C: Syslog. Lists the available SEL-FLT and SEL-FLR Syslog messages for local and remote notification.

Appendix D: Link Budget Analysis. Explains calculations of path losses for a radio link and how to determine suitable antenna type and mounting height.

Appendix E: X.509. Describes the SEL-FLR security certificates for the Ethernet and wireless interfaces.

Appendix F: Configuring Windows Network Parameters. Describes how to configure the IP address for a network connection to a PC.

Appendix G: Acronym List. Lists abbreviations commonly used in this instruction manual.

Appendix H: SEL-FLR Enclosure. Provides layout, installation, and connection information for the SEL-FLR enclosure.

Glossary. Provides definitions of various technical terms used in this instruction manual.

Safety Information

Dangers, Warnings, and Cautions

This manual uses three kinds of hazard statements, defined as follows:

⚠DANGER
Indicates an imminently hazardous situation that, if not avoided, **will** result in death or serious injury.

⚠WARNING
Indicates a potentially hazardous situation that, if not avoided, **could** result in death or serious injury.

⚠CAUTION
Indicates a potentially hazardous situation that, if not avoided, **may** result in minor or moderate injury or equipment damage.

Safety Symbols

The following symbols are often marked on SEL products.

	**⚠CAUTION** Refer to accompanying documents.	**⚠ATTENTION** Se reporter à la documentation.
	Protective earth (ground)	Terre de protection
	Direct current	Courant continu
	Instruction manual	Manuel d'instructions

Safety Marks

The following statements apply to this device.

General Safety Marks

⚠CAUTION There is danger of explosion if the battery is incorrectly replaced. Replace only with Rayovac no. BR1632 or equivalent recommended by manufacturer. See Owner's Manual for safety instructions. The battery used in this device may present a fire or chemical burn hazard if mistreated. Do not recharge, disassemble, heat above 100°C or incinerate. Dispose of used batteries according to the manufacturer's instructions. Keep battery out of reach of children.	**⚠ATTENTION** Une pile remplacée incorrectement pose des risques d'explosion. Remplacez seulement avec un Rayovac no BR1632 ou un produit équivalent recommandé par le fabricant. Voir le guide d'utilisateur pour les instructions de sécurité. La pile utilisée dans cet appareil peut présenter un risque d'incendie ou de brûlure chimique si vous en faites mauvais usage. Ne pas recharger, démonter, chauffer à plus de 100°C ou incinérer. Éliminez les vieilles piles suivant les instructions du fabricant. Gardez la pile hors de la portée des enfants.
For use in Pollution Degree 2 environment.	Pour l'utilisation dans un environnement de Degré de Pollution 2.
Terminal Ratings Wire Material Use 75°C (167°F) copper conductors only. Tightening Torque Terminal Blocks: 0.79 Nm (7 in-lb)	Spécifications des bornes Type de filage Utiliser seulement conducteurs en cuivre 75°C (167°F). Couple de serrage Borniers : 0,79 Nm (7 livres-pouce)
The separate protective earthing terminal shall be permanently connected to earth.	Courant de fuite éléve. Raccordement à la terre indispensable avant le raccordement au réseau.

Other Safety Marks (Sheet 1 of 2)

⚠DANGER Disconnect or de-energize all external connections before opening this device. Contact with hazardous voltages and currents inside this device can cause electrical shock resulting in injury or death.	**⚠DANGER** Débrancher tous les raccordements externes avant d'ouvrir cet appareil. Tout contact avec des tensions ou courants internes à l'appareil peut causer un choc électrique pouvant entraîner des blessures ou la mort.
⚠DANGER Contact with instrument terminals can cause electrical shock that can result in injury or death.	**⚠DANGER** Tout contact avec les bornes de l'appareil peut causer un choc électrique pouvant entraîner des blessures ou la mort.
⚠DANGER Install fault and load transmitters in accordance with normal safe operating procedures. These instructions are not intended to replace or supersede existing safety or operating requirements. Only trained qualified personnel with knowledge of high voltage should install or operate fault and load transmitters.	**⚠DANGER** Installez les transmetteurs de défaut et de charge conformément aux procédures normales de fonctionnement en toute sécurité. Ces instructions ne sont pas destinées à remplacer les exigences de sécurité ou de fonctionnement existantes. Seul des personnes qualifiées connaissant les équipements haute tension doivent installer ou utiliser des transmetteurs de défaut et de charge.
⚠WARNING Use of this equipment in a manner other than specified in this manual can impair operator safety safeguards provided by this equipment.	**⚠AVERTISSEMENT** L'utilisation de cet appareil suivant des procédures différentes de celles indiquées dans ce manuel peut désarmer les dispositifs de protection d'opérateur normalement actifs sur cet équipement.
⚠WARNING Have only qualified personnel service this equipment. If you are not qualified to service this equipment, you can injure yourself or others, or cause equipment damage.	**⚠AVERTISSEMENT** Seules des personnes qualifiées peuvent travailler sur cet appareil. Si vous n'êtes pas qualifiés pour ce travail, vous pourriez vous blesser avec d'autres personnes ou endommager l'équipement.
⚠WARNING Do not perform any procedures or adjustments that this instruction manual does not describe.	**⚠AVERTISSEMENT** Ne pas appliquer une procédure ou un ajustement qui n'est pas décrit explicitement dans ce manuel d'instruction.
⚠WARNING Atmospheric electrical charge accumulation can cause potential between the conductor and shield of the feed line, or cause lightning to strike an antenna. A lightning protector should be installed to prevent damage to equipment or injury to personnel.	**⚠AVERTISSEMENT** L'accumulation de charges électriques de type atmosphérique peut être la cause d'une différence de potentiel entre le conducteur et le blindage de la ligne d'alimentation ou peut attirer la foudre sur l'antenne. Un parafoudre devrait être installé pour prévenir les dommages à l'équipement ou les blessures au personnel.
⚠WARNING This device is shipped with default passwords. Default passwords should be changed to private passwords at installation. Failure to change each default password to a private password may allow unauthorized access. SEL shall not be responsible for any damage resulting from unauthorized access.	**⚠AVERTISSEMENT** Cet appareil est expédié avec des mots de passe par défaut. A l'installation, les mots de passe par défaut devront être changés pour des mots de passe confidentiels. Dans le cas contraire, un accés non-autorisé á l'équipement peut être possible. SEL décline toute responsabilité pour tout dommage résultant de cet accés non-autorisé.

Other Safety Marks (Sheet 2 of 2)

⚠CAUTION Although the power level is low, concentrated energy from a directional antenna may pose a health hazard. Do not allow users to come within 23 cm (9 in) of the antenna when the transmitter is operating in indoor or outdoor environments.	**⚠ATTENTION** Bien que le niveau de puissance soit bas, l'énergie concentrée d'une antenne directionnelle peut être un danger pour la santé. Ne pas autoriser les usagers à s'approcher à moins de 23 cm (9 po) de l'antenne quand l'émetteur est en opération dans un environnement intérieur ou extérieur.
⚠CAUTION Equipment components are sensitive to electrostatic discharge (ESD). Undetectable permanent damage can result if you do not use proper ESD procedures. Ground yourself, your work surface, and this equipment before removing any cover from this equipment. If your facility is not equipped to work with these components, contact SEL about returning this device and related SEL equipment for service.	**⚠ATTENTION** Les composants de cet équipement sont sensibles aux décharges électrostatiques (DES). Des dommages permanents non-décelables peuvent résulter de l'absence de précautions contre les DES. Raccordez-vous correctement à la terre, ainsi que la surface de travail et l'appareil avant d'en retirer un panneau. Si vous n'êtes pas équipés pour travailler avec ce type de composants, contacter SEL afin de retourner l'appareil pour un service en usine.
⚠CAUTION In order to avoid losing system logs on a factory-default reset, configure the SEL-FLR to forward Syslog messages.	**⚠ATTENTION** Pour éviter de perdre les enregistrements du système sur un redémarrage défini par défaut, configurer le SEL-FLR pour envoyer les messages de l'enregistreur du système (“Syslog”).

Wireless Regulatory Statements

The SEL-FLT and SEL-FLR are approved for use only with specific output power configurations that have been tested and approved. Modifications to the SEL-FLT, the SEL-FLR, the antenna system, and the power output that have not been explicitly specified by the manufacturer are not permitted and may render the radio noncompliant with applicable regulatory authorities. The radio equipment described in this manual emits radio frequency energy. Professional installation is required.

United States (FCC)

This equipment has been tested and found to comply with the limits for Class A digital devices, pursuant to FCC Part 15 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 radiates radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication. Operation of this equipment in a residential environment is likely to cause harmful interference, in which case the user will be required to correct the interference at his/her own expense.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Brazil

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

Este produto não é apropriado para uso em ambientes domésticos, pois poderá causar interferências eletromagnéticas que obrigam o usuário a tomar medidas necessárias para minimizar estas interferências.

Canada

English

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference that may cause undesired operation of the device.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

The radio transmitter described herein (IC ID: 4468A-900FLTR) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

French

Ce dispositif conforme aux normes CNR du gouvernement du Canada pour les appareils exempts de licence. Son utilisation est soumise à deux conditions: (1) ce dispositif ne peut causer des interférences, (2) cet appareil doit accepter toute interférence pouvant causer un mauvais fonctionnement du dispositif.

En vertu des règlements d'Industrie Canada, cet émetteur radio ne peut fonctionner avec une antenne d'un type et un maximum (ou moins) approuvés pour gagner de l'émetteur par Industrie Canada. Pour réduire le risqué d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisies de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.

L'émetteur radio décrit ci-après (IC ID: 4468A-900FLTR) a été approuvé par Industrie Canada pour fonctionner avec les types d'antennes énumérées ci-dessous avec le gain maximal admissible et nécessaire antenne d'impédance pour chaque type d'antenne indiqué. Types d'antennes ne figurent pas dans cette liste, ayant un gain supérieur au gain maximum indiqué pour ce type, sont strictement interdites pour une utilisation avec cet appareil.

General Information

Examples

This instruction manual uses several example illustrations and instructions to explain how to effectively operate the SEL-FLT and SEL-FLR. These examples are for demonstration purposes only; the firmware identification information and settings values included may not necessarily match those in your SEL-FLT or SEL-FLR.

Typographic Conventions

The instructions in this manual indicate these options with specific font and formatting attributes. The following table lists these conventions:

Example	Description
STATUS	Commands, command options, and command variables typed at a command line interface on a PC.
n	Variables determined based on an application.
<Enter>	Single keystroke on a PC keyboard.
<Ctrl+D>	Multiple/combination keystroke on a PC keyboard.
Start > Settings	PC software dialog boxes and menu selections. The > character indicates submenus.
ENABLE	Front- or rear-panel labels.

Trademarks

Trademarks appearing in this manual are shown in the following table.

AutoRANGER®	SEL Engineering Services®, Inc.
Connectorized®	

Copyrighted Software

The product includes copyrighted software licensed under the TI BSD End User Agreement, reproduced as follows:

Software License Agreement

Copyright © 2014 Texas Instruments Incorporated - http://www.ti.com/

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Texas Instruments Incorporated nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please 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

This page intentionally left blank

SECTION 1

Introduction and Specifications

Overview

Figure 1.1 SEL-FLT Fault and Load Transmitter and SEL-FLR Fault and Load Receiver

The SEL-FLT Fault and Load Transmitter and the SEL-FLR Fault and Load Receiver act in unison to comprise the SEL Wireless Line Sensor System for overhead distribution circuits. The system provides fault detection and accurate load data to a centralized location, such as a SCADA system or an outage management system (OMS). The SEL-FLT and SEL-FLR communicate with a purpose-built wireless protocol optimized for fault monitoring applications.

The SEL-FLT is a line-powered device (with battery backup) with a rugged design that meets the IEEE 495-2007 standard for faulted circuit indicators. The single shotgun-style hot stick installation and clamp allow for a quick installation that securely attaches the sensor to an overhead conductor. The multifunctional display features six ultra-bright LEDs that allow for fast local device interpretation.

The SEL-FLR serves as the access point to the SEL Wireless Line Sensor System for overhead distribution circuits. The SEL-FLR coordinates the wireless network operation and also provides the management interface for the SEL-FLT devices. The SEL-FLR also supports over-the-air firmware upgrades and settings changes to the joined SEL-FLT devices. Integration to client devices is simple through the use of Distributed Network Protocol (DNP3) via two rear-panel Ethernet ports on the SEL-FLR. The SEL-FLR also provides Syslog server functionality.

System Features and Benefits

The SEL Wireless Line Sensor System collects line sensor data and sends the information to a remote SCADA system via DNP3 messages. This allows utilities to pinpoint faulted branches on distribution circuits faster and monitor load fluctuation of a distribution circuit.

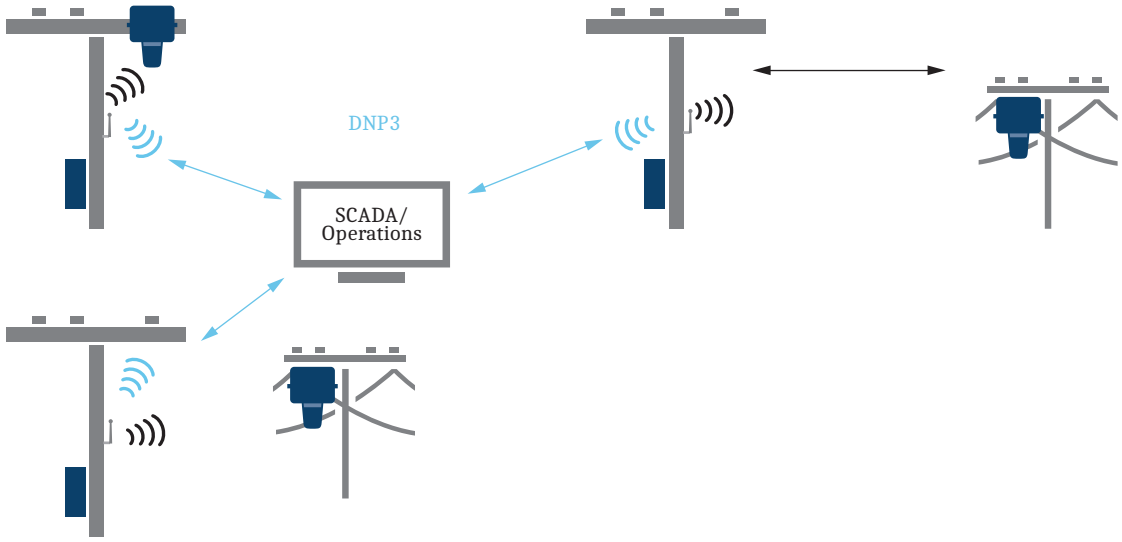
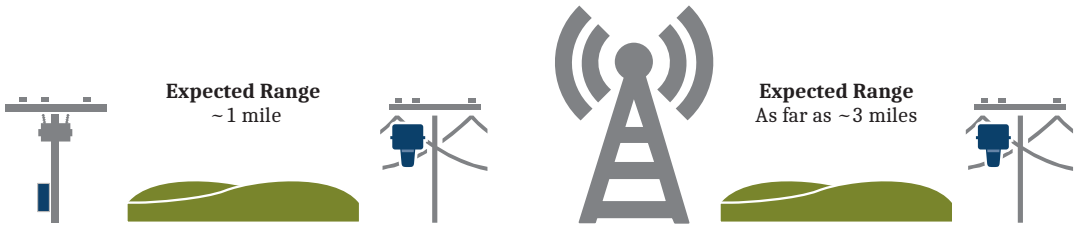


Figure 1.2 System Overview

The SEL-FLR, typically installed in a pole-mounted enclosure, receives the fault and load status from several SEL-FLT devices. The wireless communications traffic is protected by security certificates unique to each SEL-FLT. The SEL-FLR passes the aggregated sensor data via DNP3 protocol through a wired or wireless network to the central SCADA master. The SEL-FLT devices also report load information as frequently as every 5 minutes for near-real-time load monitoring.

The range of the SEL-FLT varies depending on a variety of factors including line-of-sight, sensor and antenna heights, and interference from other 900 MHz radio networks. All SEL-FLT links require onsite analysis and testing to determine with certainty if the links will be effective, but *Figure 1.3* shows the general effectiveness for SEL-FLT/SEL-FLR System links depending on the circumstances.



Radio maximum range with no obstructions to the Frensel zone: 10 miles

All links require direct line of sight and minimal interference to achieve stated performance.
Onsite testing is required for all SEL-FLT/SEL-FLR System links.

Figure 1.3 Line-of-Sight Range for Typical Wireless Applications

The rugged design and wide operating temperature range of the SEL-FLR allow for installation in pole-mounted control enclosures, substation control houses, and communication tower control houses. Installing the SEL-FLR in a pole mounted enclosure helps achieve optimal wireless connectivity to nearby SEL-FLT devices.

In addition to sending DNP3 data to SCADA systems, the SEL-FLR is equipped with a powerful web-based user interface for setting up the network, viewing data, and troubleshooting. The SEL-FLR web interface (as shown in *Figure 1.8*) manages all of the SEL-FLT settings and over-the-air firmware upgrades.

The SEL-FLR accumulates diagnostic information from its own system, as well as diagnostic, fault, and load information from joined SEL-FLT devices. You can access the accumulated information either locally via an Ethernet connection or remotely through a wired or wireless network connection.

Product Overview

SEL-FLT Product Overview

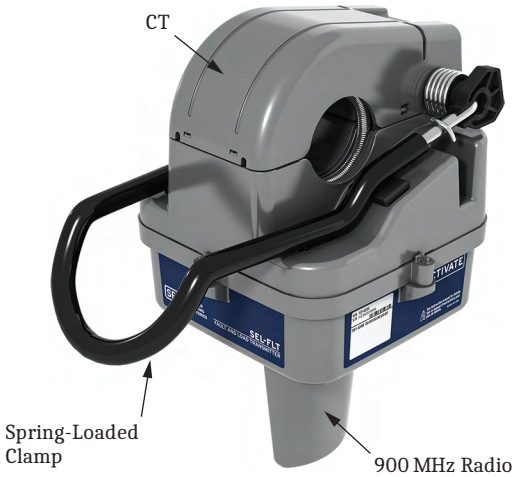


Figure 1.4 SEL-FLT Characteristics (Front)

Spring-Loaded Clamp

The spring-loaded clamp simplifies installation on overhead conductors and holds the SEL-FLT in position. See *SEL-FLT Installation* on page 2.11 for more information.

Integrated Radio

The 900 MHz radio module is mounted inside the SEL-FLT cone for environmental protection. The radio communicates to a single SEL-FLR to transmit fault and load data. See *Section 4: SEL-FLR Configuration* for more information.

Current Transformer (CT)

The SEL-FLT split-core CT harvests energy to power the device and accurately detects fault and load data. See *Section 7: SEL-FLT Features* for information about device powering, and *SEL-FLT Load Monitoring* on page 7.9 and *SEL-FLT Fault Detection* on page 8.7 for more information about detecting faults and load data.

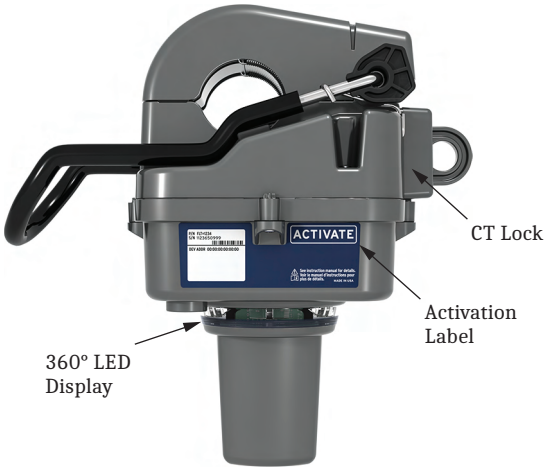


Figure 1.5 SEL-FLT Characteristics (Side)

LED Display

The SEL-FLT is equipped with a local LED display that provides the indication of different events and device statuses. See *SEL-FLT Local Display* on page 7.6 for more information.

Locking Mechanism

The SEL-FLT CT lock ensures the CT remains securely closed when the product is installed. See *Section 7: SEL-FLT Features* for more information on the CT lock.

Device Activation

Device wake-up, radio activation, and device reset on the SEL-FLT are all accomplished via use of a magnet tool. See *Section 7: SEL-FLT Features* for more information on the magnet tool operations.

SEL-FLR Front-Panel Overview

Figure 1.6 SEL-FLR Front Panel

Device Status LEDs

The **ENABLED** LED is illuminated green when the unit is operational. This LED is unlit during startup. The **ALARM** LED illuminates when the unit asserts an alarm. The alarm status LED is described in more detail in *Section 6: Diagnostics*.

Port Activity and Radio Status Indicator LEDs

Each of the two rear-panel Ethernet ports has a pair of corresponding LED indicators on the front panel (labeled **1** and **2**): the yellow 100 Mbps LED indicates port speed, and the green LINK/ACT LED indicates link activity. Refer to *Ethernet Network Interfaces* on page 4.15 for more information.

The radio status LEDs (on the right side of the front panel) indicate radio and SEL-FLT network status as follows:

- The green **LINK** LED indicates that at least one SEL-FLT is wirelessly joined with the SEL-FLR.
- The green **ACT** (activity) LED illuminates each time the SEL-FLR receives data from an SEL-FLT.
- The four-segment multicolored **LINK QUALITY** indicator represents the received signal quality for each SEL-FLT message received on the wireless network.

For more information on radio status indicators, see *Radio Network* on page 4.1.

Local Management Port

The front panel includes an RJ45 Ethernet port for local device management, settings, and commissioning. For more information, see *Ethernet Network Interfaces* on page 4.15.

Pinhole Reset

The front panel includes a pinhole reset with two functions: the first is to reenable front-panel Port F (**ETH F**) functionality, and the second is to reset the SEL-FLR to factory defaults (see *Device Reset* on page 5.18).

SEL-FLR Rear-Panel Overview

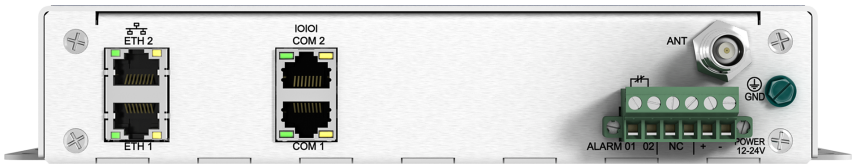


Figure 1.7 SEL-FLR Rear Panel

Ethernet Ports

The two rear-panel Ethernet ports support 10/100 Mbps and work together as an unmanaged switch. Both ports use RJ45 connections for Ethernet over copper cabling. See *Ethernet Network Interfaces* on page 4.15 for more information.

Alarm Contact

The rear-panel connector provides one Form B alarm contact. This contact provides notification to various alarms on the system. The alarm contact is described in more detail in *SEL-FLR Alarms* on page 6.1.

Power Supply Input

The rear-panel connector accepts power from a 9–30 Vdc power source. See *SEL-FLR Specifications* on page 1.11 for power supply ratings.

TNC Antenna Input

The SEL-FLR is equipped with a TNC antenna input port. For more information about antennas and cabling options, see *SEL-FLR Installation and Connections* on page 2.6.

Grounding Lug

A grounding lug is located on the right side of the rear panel. See *SEL-FLR Installation and Connections* on page 2.6 for grounding instructions.

SEL-FLR Web Interface

Commission and manage the SEL-FLR through the use of the web interface. Secure access is controlled through the use of X.509 certificates and user-based accounts stored locally on the device. The device interface includes a dashboard display of all radio and sensor diagnostics, as shown in *Figure 1.8*.

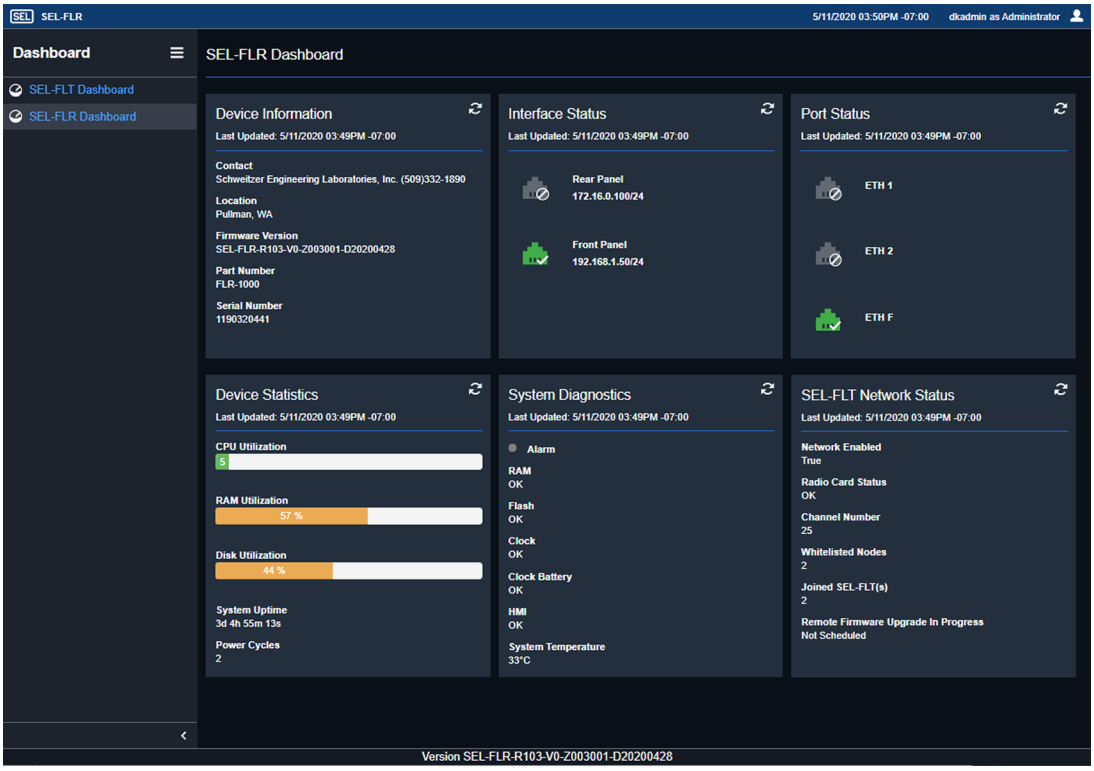


Figure 1.8 Dashboard Display

Models, Options, and Accessories

Models

Table 1.1 SEL-FLT and SEL-FLR Models by Country

Countries	SEL-FLT	SEL-FLR
U.S.A., Canada, Mexico	FLT-1000	FLR-1000
Peru	FLT-1003	FLR-1003
Brazil	FLT-1006	FLR-1006
Costa Rica	FLT-1007	FLR-1007
Argentina	FLT-1008	FLR-1008
Ecuador	FLT-1009	FLR-1009

Accessories

Table 1.2 SEL-FLT Orderable Accessories

Description	Part Number
Magnet Tool	CRSRTT
Mini Current Loop	MCL120

Table 1.3 SEL-FLR Orderable Accessories (Sheet 1 of 2)

Description	Part Number
Feed Line	
LMR-400 TNC Male to N Male Cable	SEL-C966
LMR-400 N Male to N Male Cable	SEL-C968
7/8" Heliax N Male to N Male Cable	SEL-C978
N Female to TNC Male Adapter	240-1809
900 MHz Pole-Top Omnidirectional Antennas[a]	
Low-Profile 3 dBi Omnidirectional, N Female Connector	235-0003
Vertical 7.15 dBi Omnidirectional, N Female Connector	235-0232
Vertical 9.15 dBi Omnidirectional, N Female Connector	235-0233
900 MHz Base Station Omnidirectional Antennas[a]	
Vertical 8.1 dBi Omnidirectional, N Female Connector	235-0234
900 MHz Yagi Directional Antennas[a]	
3-Element 8.5 dBi Yagi, N Female Connector	235-0221
5-Element 11.1 dBi Yagi, N Female Connector	235-0220
11-Element 14.1 dBi Yagi, N Female Connector	235-0222
900 MHz Indoor Antennas[a]	
Indoor 20.32 cm (8 in) Omnidirectional, TNC Male Connector	235-0108
Antenna Mounting Hardware	
Yagi Mount for 4.8 cm (1.9 in) Maximum Diameter Poles	Included With Yagi Antenna Purchase
Vertical Omnidirectional Mount for 35.56 cm (14 in) Maximum Diameter Poles	240-0103

Table 1.3 SEL-FLR Orderable Accessories (Sheet 2 of 2)

Description	Part Number
Yagi Mount for 35.56 cm (14 in) Maximum Diameter Poles	240-0104
Mast Mount for Omnidirectional Antennas (6.35 cm [2.5 in] Maximum Diameter Mast)	240-0106
Power Supply	
15 Vdc Power Supply	SEL-9322
15 Vdc Power Supply, 120–240 Vac Input With Tinned Leads	230-0604
Surge Protection	
Radio Surge Protector With N Female Connectors	200-2004
In-Line Grounding Cable	240-0124

[a] Not certified for Brazil (model FLR-1006). Contact SEL for approved antenna models.

SEL-FLT Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

General

Operating Temperature Range:	–40° to +85°C (–40° to +185°F)
Storage Temperature Range:	–40° to +85°C (–40° to +185°F)
Operating Environment	
Pollution Degree:	2
Relative Humidity:	5%–95%, noncondensing
Maximum Altitude:	2000 m (6562 ft)
Ingress Protection:	IP-66
Clamp Range:	6.4–38.1 mm (0.25–1.50 in)
Dimensions:	159 mm x 192 mm x 252 mm (6.3 in x 7.6 in x 9.9 in)
Weight:	1.6 kg (3.6 lb)

System

Frequency Range:	50–60 Hz
Current Range:	3–600 A
Maximum Voltage:	69 kV (line-to-line)

Fault Detection

Trip Threshold Range:	25–1600 A
Fault Detection Accuracy:	±(2 A + 4%)
Maximum Fault Current:	25 kA for 10 cycles
Trip Response Time:	24 ms at 60 Hz (default)

Load Measurement

Current Range:	3–600 A
Measurement Accuracy:	±(0.25 A + 1%) from 5–600 A (typical) ±(2.5 A + 2%) from 5–600 A (maximum) ±3 A from 3–5 A (maximum)

Power

Minimum Continuous Operating Current:	3.5 A (AutoRange) 4 A (Fixed Trip)
Battery Capacity:	19 Ah
Battery Shelf-Life:	20 years

Flash Hours

Harvested Power Flash Time:	8 hours (per outage)
Battery Flash Time:	1800 hours

Radio

Frequency Band	
FLT-1000 (U.S.A., Canada, Mexico):	902–928 MHz ISM, 25 non-overlapping channels
FLT-1003 (Peru):	916–928 MHz, 11 non-overlapping channels
FLT-1006 (Brazil):	902–907 MHz and 915–928 MHz, 16 non-overlapping channels
FLT-1007 (Costa Rica):	921–928 MHz, 6 non-overlapping channels
FLT-1008 (Argentina):	902–928 MHz ISM, 25 non-overlapping channels
FLT-1009 (Ecuador):	915–928 MHz, 12 non-overlapping channels
Occupied Bandwidth:	850 kHz
Modulation:	Digital modulation 2-FSK
Operating Mode:	Point-to-multipoint
Power Output:	0.4 W (26 dBm)
Sensitivity:	–102 dBm ± 2 dB at 5% PER
Fixed Antenna Gain:	–4 dBi
Polarization:	Vertical
Link Data Rate:	62.5 kbps
Typical Effective Line-of-Sight Range	
Receiver Antenna Mounted on a Distribution Pole:	Approximately 1 mile[a]
Receiver Antenna Mounted on a 75 ft Communications Tower:	Approximately 3 miles[a]
Radio Maximum Range With No Obstructions:	Up to 10 miles

[a] Requires flat terrain with clear line of sight and no RF interference—see *SEL-FLT/SEL-FLR System Deployment Guide* for details.

Error Detection:	16-bit CRC
Encryption:	AES 128-bit

Type Tests

Environmental Tests

Temperature Cycling:	IEEE 495-2007 Test 4.4.1; 2 hours at –40°, +20°, and +85°C, 5 cycles
Trip Current:	IEEE 495-2007 Test 4.4.9; –30°, +20°, and +70°C
Reset:	IEEE 495-2007 Test 4.4.10; –30°, +20°, and +70°C
Short-Time Current:	IEEE 495-2007 Test 4.4.7; 25 kA for 10 cycles
Adjacent Phase Immunity:	IEEE 495-2007 Test 4.4.8; 25 kA at 18 inches
Time Current:	IEEE 495-2007 Test 4.4.11; <1 ms
Vibration Resistance:	IEC 60255-21-1:1988 Class 2 Endurance Class 2 Response IEEE 495-2007 Test 4.4.6
Shock and Bump Resistance:	IEC 60255-21-2:1988 Class 1 Shock Withstand Class 1 Bump Class 2 Shock Response IEEE 495-2007 Test 4.4.6
Seismic Resistance:	IEC 60255-21-3:1993 Class 2 (Quake Response) IEEE 495-2007 Test 4.4.6
Salt Spray:	IEEE 495-2007 Test 4.4.4 MIL-STD-810G: Method 509.5
Cold:	IEC 60068-2-1:2007 –40°C, 16 hours

Dry Heat: IEC 60068-2-2:2007
+85°C, 16 hours

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

Damp Heat, Steady State: IEC 60068-2-78: 2012
+40°C, 93% relative humidity

Outdoor Weathering: IEEE 495-2007
Test 4.4.3
ASTM G154-16

Ingress Protection: IP-66

Rain: MIL-STD-810G: Method 506.5
Procedure 1 Rain and Blowing Rain

Ice Build-Up: MIL-STD-810G: Method 521.4
Procedure 1

Electromagnetic Compatibility Immunity

Electrostatic Discharge Immunity: IEC 60255-26:2013
Severity Level 4
8 kV contact discharge
15 kV air discharge
IEC 61000-4-2:2009
Severity Level 4
8 kV contact discharge
15 kV air discharge
IEEE C37.90.3-2001
Severity Level 3
8 kV contact discharge
15 kV air discharge

Radiated RF Immunity: EN 60255-26:2013
10 V/m
EN 61000-4-3:2006+A1:2008+A2:2010
10 V/m
IEEE C37.90.2-2004
35 V/m

Power Frequency Magnetic Field Immunity: IEC 60255-26:2013
1000 A/m for 3 seconds
100 A/m for 1 minute
IEC 61000-4-8:2009
1000 A/m for 3 seconds
100 A/m for 1 minute

Pulse Magnetic Field Immunity: IEC 61000-4-9:2016
1000 A/m

Damped Oscillatory Magnetic Field Immunity: IEC 61000-4-10:2016
100 A/m

Electromagnetic Compatibility Emissions

Radiated RF Emissions: IEC 60255-26:2013
FCC Part 15.247; ICES-001; RSS-210

Certifications

Table 1.4 SEL-FLT Certifications by Country

Country	SEL-FLT Model Number	Authority	Reference
U.S.A.	FLT-1000	FCC	R34-900FLTR
Canada	FLT-1000	IC	4468A-900FLTR
Mexico	FLT-1000	IFETEL	RCPSCSE20-0664
Peru	FLT-1003	MTC	TRSS43952
Brazil	FLT-1006	Anatel	05384-20-12987
Costa Rica	FLT-1007	SUTEL	
Argentina	FLT-1008	ENACOM	C-27030
Ecuador	FLT-1009	ARCOTEL	ARCOTEL-NRH-2020-000625

SEL-FLR Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

General

SEL-FLR

Temperature Range:	–40° to +85°C (–40° to +185°F) per IEC 60068-2-1 and 60068-2-2

SEL-FLR Enclosure

With SEL-3061:	–25° to +50°C (–13° to +122°F)
Max. Loading (SEL-3061 and <10 W of Accessories):	–25° to +40°C (–13° to +104°F)
Without Direct Sunlight:	Increase max. temperatures by 15°C (27°F)

Operating Environment

Pollution Degree:	2
Relative Humidity:	5%–95%, noncondensing
Maximum Altitude:	2000 m (6562 ft)
SEL- FLR Dimensions:	216 mm x 165.1 mm x 44.5 mm (8.5 in x 6.5 in x 1.75 in)
SEL-FLR Enclosure Dimensions:	685.8 mm x 405.7 mm x 276.5 mm (27.0 in x 15.97 in x 10.89 in)
SEL-FLR Weight:	1 kg (2.2 lb)
SEL-FLR Enclosure Weight (Without Batteries):	13.3 kg (29.5 lb)
RF Connector:	TNC
Supported Web Browser:	Google Chrome

Communications (Ethernet)

Ports:	2 rear, 1 front
Data Rate:	10/100 Mbps
Rear Connectors:	RJ45
Standard:	IEEE 802.3

Power Supply

SEL-FLR

Input Voltage Range:	9–30 Vdc
Power Consumption:	<10 W

SEL-FLR Enclosure

Input Voltage:	120 Vac nominal
AC Power Consumption:	<39 W
Usable DC Load:	<25 W

Radio

Frequency Band

FLR-1000 (U.S.A., Canada, Mexico):	902–928 MHz ISM, 25 non-overlapping channels
FLR-1003 (Peru):	916–928 MHz, 11 non-overlapping channels
FLR-1006 (Brazil):	902–907 MHz and 915–928 MHz, 16 non-overlapping channels
FLR-1007 (Costa Rica):	921–928 MHz, 6 non-overlapping channels
FLR-1008 (Argentina):	902–928 MHz ISM, 25 non-overlapping channels
FLR-1009 (Ecuador):	915–928 MHz, 12 non-overlapping channels
Occupied Bandwidth:	850 kHz
Modulation:	Digital modulation 2-FSK
Operating Mode:	Point-to-multipoint
Power Output:	0.4 W (26 dBm)
Sensitivity:	–102 dBm ± 2 dB at 5% PER
Polarization:	Vertical
Link Data Rate:	62.5 kbps

Typical Effective Line-of-Sight Range

Receiver Antenna Mounted on a Distribution Pole:	Approximately 1 mile[a]
Receiver Antenna Mounted on a 75 ft Communications Tower:	Approximately 3 miles[a]
Radio Maximum Range With No Obstructions:	Up to 10 miles

[a] Requires flat terrain with clear line of sight and no RF interference—see *SEL-FLT/SEL-FLR System Deployment Guide* for details.

Error Detection:	16-bit CRC
Encryption:	AES 128-bit

Alarm Output

Rated Operational Voltage:	24–250 Vdc
Contact Protection:	300 Vdc, MOV-protected
Continuous Carry:	2 A
Pickup Time:	≤8 ms typical
Dropout Time:	≤8 ms typical

Type Tests

Communications Equipment Tests

Communications for Substation Equipment:	IEEE 1613-2009 Class 1
Power Frequency Disturbances:	IEC 61850-3:2002

Environmental Tests

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

Safety

Measuring Relays and Protection Equipment: IEC 60255-27:2013

Protection IP Code: IEC 60529:2001
IP Code: IP3X for category 2 equipment

Insulation Coordination: IEC 60255-27:2013
IEEE C37.90-2005
Dielectric (HiPot) Severity Level:
Power Supply: 3100 Vdc
Alarm Contact: 2500 Vac
Impulse Severity Level:
5 J; ±5 kV, 1.2/50 ms
2.4 kV on Ethernet Port
IEEE 802.3-2012
Ethernet ports comply with Environment A requirements

Electromagnetic Compatibility Immunity Tests

Electrostatic Discharge Immunity: IEC 60255-26:2013
Severity Level 4
8 kV contact discharge
15 kV air discharge
IEC 61000-4-2:2009
Severity Level 4
8 kV contact discharge
15 kV air discharge
IEEE C37.90.3-2001
Severity Level 3
8 kV contact discharge
15 kV air discharge

Conducted RF Immunity: IEC 60255-26-6:2013
10 Vrms
IEC 61000-4-6:2008
10 Vrms

Radiated RF Immunity: EN 60255-26:2013
10 V/m
EN 61000-4-3:2006+A1:2008+A2:2010
10 V/m
IEEE C37.90.2-2004
35 V/m

Electrical Fast Transient Burst Immunity: IEC 60255-26:2013
4 kV @ 5.0 kHz for power port
2 kV @ 5.0 kHz for communications ports
IEC 61000-4-4:2012
4 kV @ 5.0 kHz for power port
2 kV @ 5.0 kHz for communications ports

Power Frequency Magnetic Field Immunity: IEC 60255-26:2013
1000 A/m for 3 seconds
100 A/m for 1 minute
IEC 61000-4-8:2009
1000 A/m for 3 seconds
100 A/m for 1 minute

Power Supply Immunity: IEC 60255-11:2008
IEC 61000-4-11:2004
IEC 61000-4-17:1999+A1:2001 +A2:2008
IEC 61000-4-9:2000

Surge Withstand Capability Immunity: IEC 60255-26:2013
2.5 kV common mode
1 kV differential mode
IEC 61000-4-18:2006+A1:2010
2.5 kV common mode
1 kV differential mode
IEEE C37.90.1-2012
2.5 kV oscillatory
4 kV fast transient

Electromagnetic Compatibility Emissions

SEL-FLR Radiated RF Emissions: IEC 60255-26:2013
FCC Part 15.247; ICES-001; RSS-210

SEL-FLR Enclosure Radiated RF Emissions: FCC Part 15.107, 15.109; ICES-001, Issue 5

Certifications

Table 1.5 SEL-FLR Certifications by Country

Country	SEL-FLR Model Number	Authority	Reference
U.S.A.	FLR-1000	FCC	R34-900FLTR
Canada	FLR-1000	IC	4468A-900FLTR
Mexico	FLR-1000	IFETEL	RCPSCSE20-0664
Peru	FLR-1003	MTC	TRSS48383
Brazil	FLR-1006	Anatel	05385-20-12987
Costa Rica	FLR-1007	SUTEL	
Argentina	FLR-1008	ENACOM	C-26864
Ecuador	FLR-1009	ARCOTEL	ARCOTEL-NRH-2020-000626

SECTION 2

Installation

Overview

This section includes the following:

Diagram and Dimensions

SEL-FLT Dimensions

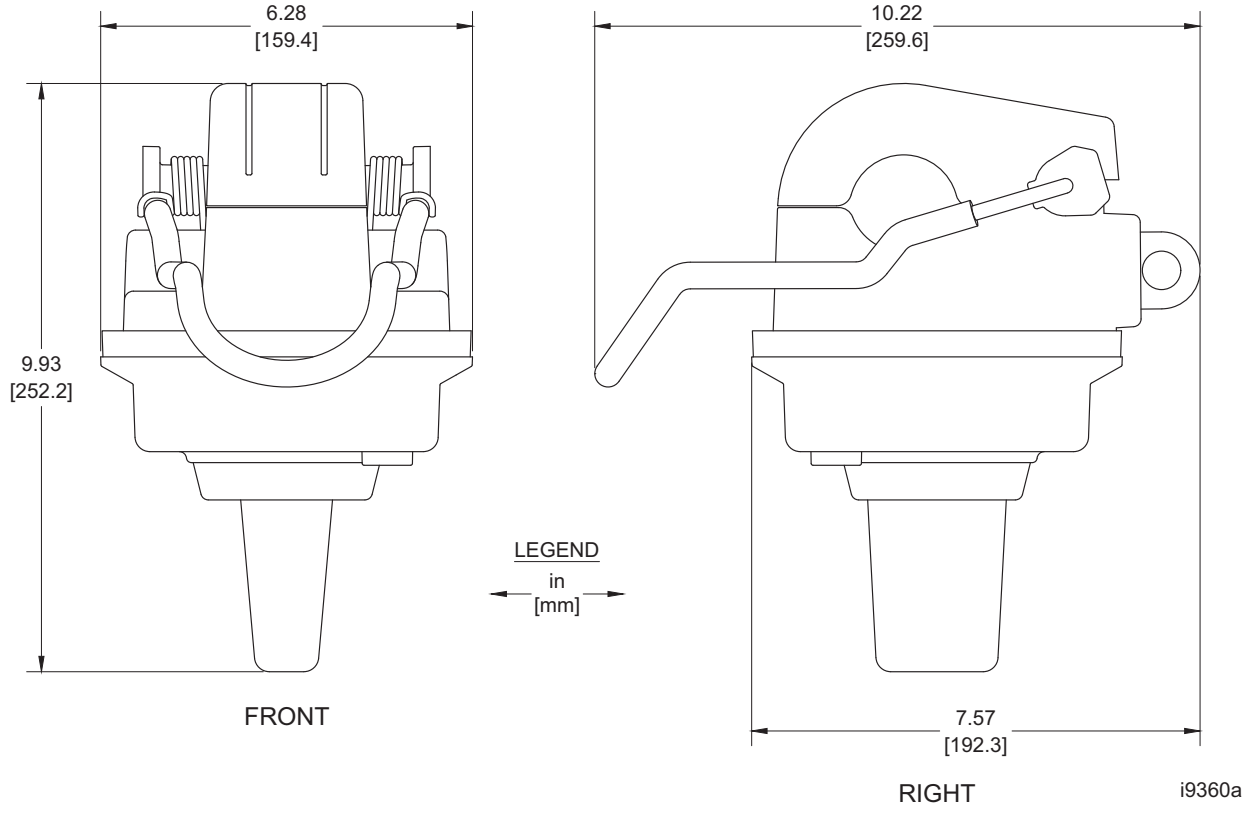


Figure 2.1 SEL-FLT Dimensions

SEL-FLR Dimensions

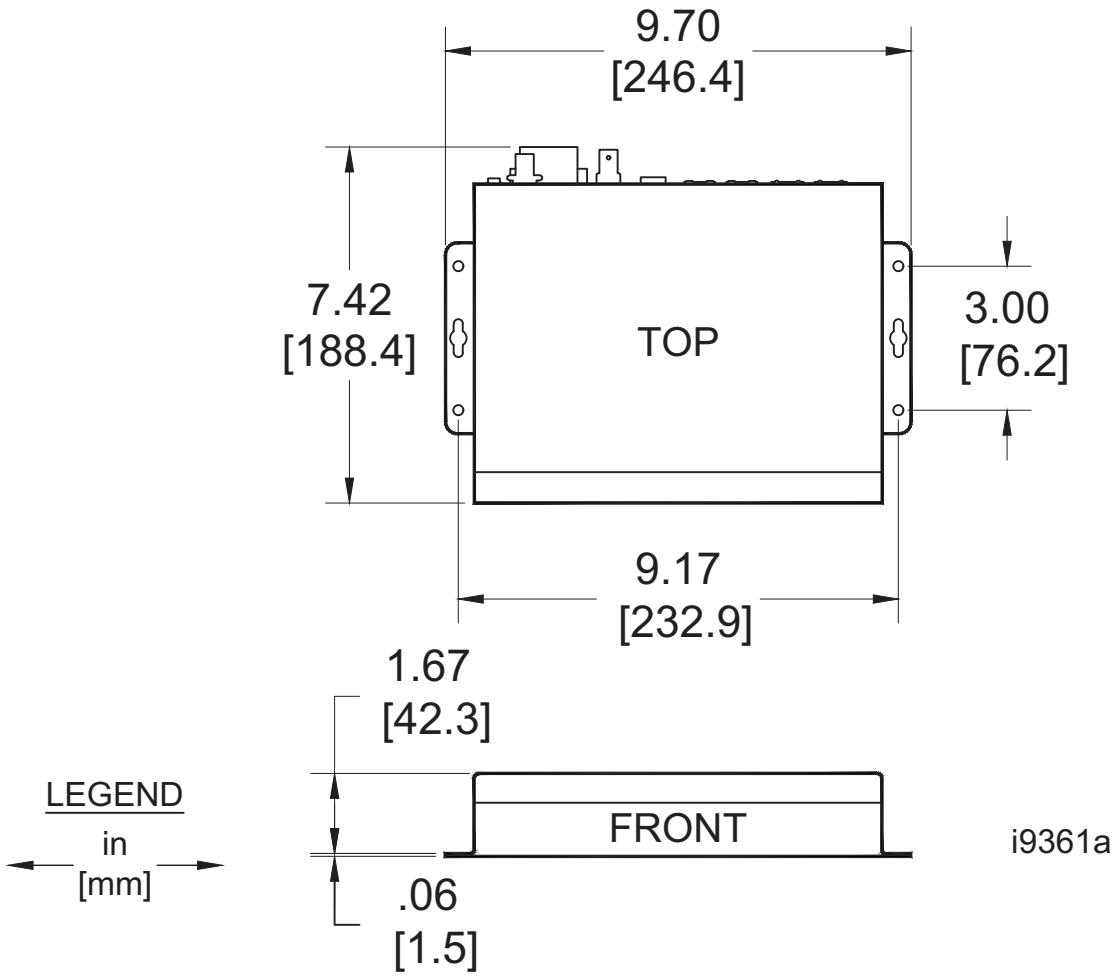


Figure 2.2 SEL-FLR Dimensions

System Deployment

The SEL-FLT and SEL-FLR system is simple to deploy at a few or several locations on your power system. This section provides details that should be considered when planning your deployment to ensure that the process proceeds smoothly. The typical deployment process will include the following phases:

- Research
  - Installation site candidate selection
  - Antenna selection
  - Link budget estimation
- Planning
  - Channel selection
  - Site survey
  - SEL-FLR communication backhaul

- Installation
  - SEL-FLR installation
  - SEL-FLR systems setup
  - SEL-FLT installation
  - SEL-FLT commissioning
- Setup
  - SEL-FLR network setup
  - SEL-FLT settings configuration

It is important to begin the system deployment process with the research and planning phases to ensure that the overall deployment proceeds smoothly. Consider the following guidelines before deploying the SEL-FLT and SEL-FLR system:

- Select SEL-FLR and SEL-FLT installation locations with a clear line of sight (i.e., minimal path obstructions) for best network performance.
- Perform a separate link budget estimation for every unique link on the network (i.e., between the SEL-FLR and each group of collocated SEL-FLT devices). See *Appendix D: Link Budget Analysis* for more information.
- Choose a network channel that has the least amount of RF interference. See *Site Analysis* on page 4.8 for details on determining the amount of RF interference.
- Avoid using radio frequencies occupied by any other utility radio equipment operating in the same area (such as SEL-3060A Ethernet Radios).
- Set a unique channel for SEL-FLR devices that operate in the same area to avoid network interference.

Research

The first step in the deployment process is to identify possible installation sites for both the SEL-FLR and SEL-FLT devices, and then determine if a reliable communication link can be established. SEL recommends deploying SEL-FLT devices so that they are visible from the SEL-FLR antenna and there are no obstructions between the two devices. The SEL-FLR enclosure provides a flexible, off the shelf solution for pole-mounting an SEL-FLR in close proximity to each group of proposed SEL-FLT installation sites. A low-gain antenna is usually acceptable for this type of deployment, but a simple link budget estimation should still be performed to determine if the link margin is acceptable (see *Appendix D: Link Budget Analysis* for details). Select an SEL-FLR antenna and feeder cable from the list shown in *Table 1.3* and include the gain and loss information for these components in the link budget analysis. Refer to the SEL-FLT/SEL-FLR System Deployment Guide for information related to deployment of longer range communication links.

When the distance between the SEL-FLR and the SEL-FLT devices is very short (7–30 m [23–100 ft]), some attenuation should be added in the line between the SEL-FLR and the antenna. This will limit the range of the SEL-FLR and will reduce RF interference to other devices. When the link budget estimate shows a receive signal strength of greater than –40 dBm, consider adding attenuation to the SEL-FLR feed line to reduce RF interference to other devices.

Planning

SEL-FLR Communication Backhaul

Communication backhaul for SEL-FLR installation sites must be considered as part of the deployment planning process. Reliable communication backhaul ensures that fault status and load measurement information from SEL-FLT devices is able to be reliably communicated to SCADA. Applications using the SEL-FLR pole-mounted enclosure typically use a cellular router, such as the SEL-3061, to securely communicate over public cellular networks, though several other options are also viable. The ability of the SEL-FLR to communicate over any backhaul that supports DNP3 protocol via ethernet provides flexibility when planning communication from the SEL-FLR to SCADA. If 900 MHz radios are selected for communication backhaul from the SEL-FLR, additional consideration should be given to potential RF interference from these devices.

Channel Selection

The SEL-FLR and SEL-FLT communicate on a channel selected from the license-free 900 MHz ISM (industrial, scientific, and medical) band. See *Table 4.2* for a list of available radio channels for each specific model.

Choose a radio channel with minimal RF interference to help ensure the best network performance. The SEL-FLR has a site analysis tool for determining the amount of RF interference on each channel (see *Site Analysis* on page 4.8 for details). When operating other 900 MHz radios that use spread spectrum or frequency hopping in the same area as the SEL-FLR, designating skip zones can help to provide channels relatively free of interference for SEL-FLR operation.

To avoid interference, set each SEL-FLR with a unique channel when multiple SEL-FLR radios are installed near one another. See *Channel Selection* on page 4.6 for details on configuring the SEL-FLR channel.

SEL-FLT Site Survey

Survey the SEL-FLT installation site to check for local obstructions between the SEL-FLT and SEL-FLR. If an obstruction does exist, consider whether the SEL-FLT location could be moved to a nearby span to avoid the obstruction without compromising the application of the device. If an alternative SEL-FLT location meeting these criteria is not available, consider whether an alternative SEL-FLR installation site would provide an unobstructed signal path without compromising communication with other SEL-FLT devices in the area. When neither of these conditions can be met, consider installation of an additional SEL-FLR installation site at a location where the signal path to the SEL-FLT devices is free from obstructions.

System Installation

SEL-FLR Installation

Install the SEL-FLR at the identified site or set of sites and enable the radio before installing any SEL-FLT devices. It is not uncommon to start with a small number of pilot installation sites in order to evaluate the SEL-FLT and SEL-FLR system and establish internal best practices for system deployment prior to installing units at all proposed sites. Follow the procedures in *SEL-FLR Installation and Connections* on page 2.6 for instructions on the physical installation. Commission the SEL-FLR as described in *Commissioning the SEL-FLR* on

page 2.22. Once logged in, follow the instructions in *SEL-FLR Radio Network Settings* on page 4.6 to turn on the SEL-FLR radio after selecting a radio channel as described in *Channel Selection* on page 2.4.

Verify the radio is enabled and functioning with a nearby SEL-FLT device (for this test, the SEL-FLT does not need to be installed on an overhead power line). Activate the radio in the SEL-FLT and verify that the device registers on the SEL-FLR Discovery list (see *Discovery list* on page 4.12). The RSSI information available will indicate the signal strength verifying RF connectivity and initial SEL-FLR setup. You are now ready to install SEL-FLT devices on the distribution system.

SEL-FLT Installation

At the installation site, activate the SEL-FLT radio by following the instructions in *SEL-FLT Wake-Up and Radio Activation* on page 2.10. Verify the RF connectivity at the local SEL-FLR. Verify that the Discovery list of the local SEL-FLR is populated with the recently activated SEL-FLT devices (see *Discovery list* on page 4.12). Install the SEL-FLT devices by following the instructions in *SEL-FLT Installation* on page 2.11. Record the location of each SEL-FLT device per the instructions in *SEL-FLT Product Identification* on page 2.10.

Verify that the installed SEL-FLT devices can communicate with the local SEL-FLR. Confirm that the RSSI information is similar to the expected signal level determined link budget analysis. Add the SEL-FLT devices to the whitelist as described in *Adding SEL-FLT Devices* on page 4.13.

These steps should be repeated for all collocated SEL-FLT installations.

System Setup

The final step of system deployment is to complete the SEL-FLR setup by performing the following:

Step 1. Enable the rear-panel interface and ports for remote access and DNP3 communications, and set up a remote Syslog destination. See *Ethernet Network Interfaces* on page 4.15 for more information.

Step 2. Set up the SEL-FLR as a DNP3 Level 2 Outstation device that can communicate with a DNP3 client. See *DNP Communication* on page 4.19 for more information.

Step 3. Set up the SEL-FLR to transmit the event messages to as many as three different remote Syslog destinations. See *Syslog Reporting* on page 6.4 for more information.

Step 4. Manage the configurable SEL-FLT settings through the SEL-FLR web interface. See *SEL-FLT Parameters and Settings* on page 4.28 for more information.

SEL-FLR Installation and Connections

The SEL-FLR features a wall-mount design for substations or downline enclosures. Before initial startup, make sure that the radio is properly grounded to the common building or enclosure ground system.

Physical Installation

You can mount the SEL-FLR in a sheltered indoor environment or in an outdoor enclosure. If mounted outdoors, the enclosure must adhere to the temperature and humidity ratings for the device, and the SEL-FLR must be protected against exposure to direct sunlight, precipitation, and full wind pressure. The SEL-FLR enclosure provides a complete solution that meets all of the requirements for mounting the SEL-FLR in outdoor environments.

Install the SEL-FLR using #6 or #8 screws. Secure the SEL-FLR by using at least four of the six mounting holes located on the tabs on the side of the device.

Antenna Mounting

See the *SEL Radio Accessories Guide* (available at selinc.com) for complete information on radio accessories.

The SEL-FLR is designed to communicate with an external antenna (see *Table 1.3* for a list of available antennas). Before choosing your antenna, make sure you understand the radio principles outlined in *Appendix D: Link Budget Analysis*. A low-gain antenna is usually acceptable for most applications.

Once you determine a link is likely to be viable, position your antenna so that it has a clear line of sight to all desired SEL-FLT devices in the immediate area. Most SEL-FLR applications will use an omnidirectional antenna. Alternatively, a directional antenna can also be used. Directional antennas ordered from SEL include pipe-mounting brackets (for pipes with a maximum diameter of 4.8 cm [1.9 in]). *Table 1.3* lists the equipment necessary for mounting omnidirectional antennas to a pipe or mounting either directional or omnidirectional antennas to a large pole.

Connections

The SEL-FLR requires a dc power supply, proper grounding, and antenna connections to properly function. Ethernet connections can be added to support DNP3 communication, remote Syslog destinations, or remote access to the SEL-FLR. Connecting the alarm contact provides the indication for major alarm events on the system. *Figure 2.3* shows an example installation.

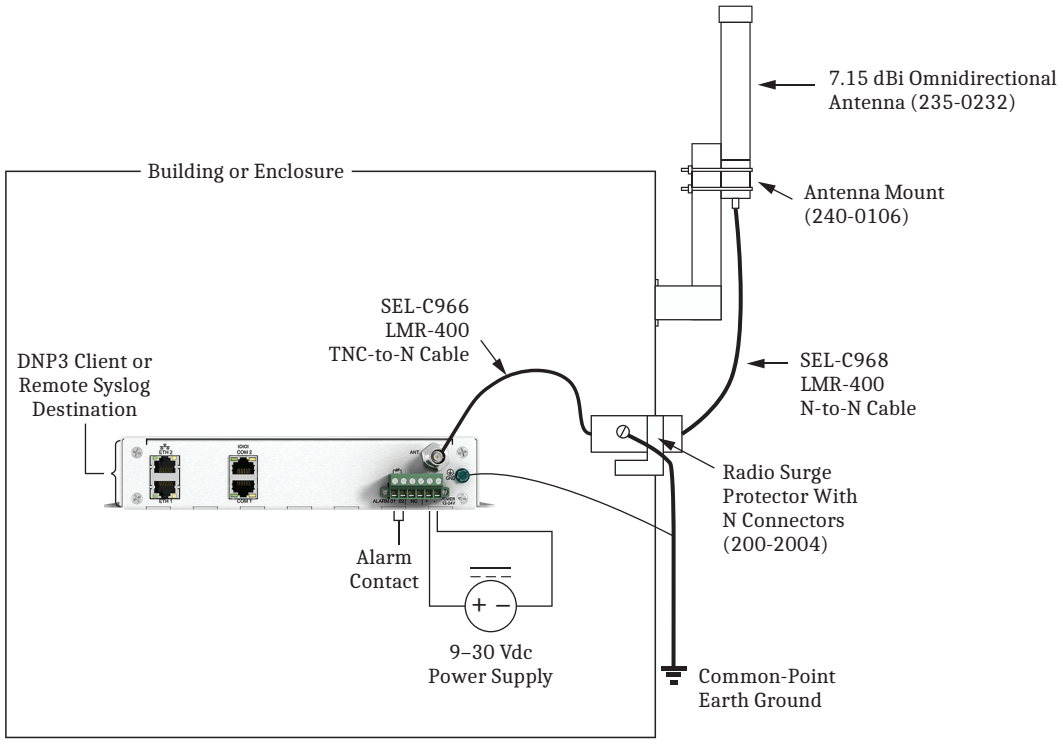


Figure 2.3 Typical SEL-FLR Installation With Surge Protection

Grounding

Ground the SEL-FLR chassis at the ground terminal located on the rear of the device. You must connect the ground terminal labeled with the ground symbol to a rack frame or switchgear ground for proper safety and performance. Use 2.5 mm^2 (14 AWG) wire less than 2 m (6.6 ft) in length. The radio ground should be connected to the same point as the surge protector ground to avoid ground-rise potential damage.

Terminal Connector

The power terminal connections and alarm contacts are located on the six-position Connectorized terminal located on the rear of the device. The two pins labeled **NC** indicate *not connected*.

For all connections to the Connectorized terminal, use a conductor size between 0.25 mm^2 (24 AWG) and 4 mm^2 (12 AWG). Strip the conductor end to 8.0 mm (0.32 in) to ensure an electrical connection is made. Insert the bare conductor into the connection and past the connection jaw, and tighten the connector to 0.79 Nm (7 in-lb) of torque. Complete all wiring connections before inserting the connector into the SEL-FLR.

Power Terminals

The power terminals, labeled **+** and **−**, must connect to a nominal 12 or 24 Vdc power source. The supply voltage range is located on the serial label on the side of the unit.

To avoid damaging the antenna port, ensure that you have a proper 50 Ω load on the antenna port before applying power to the SEL-FLR.

Antenna Port

Connect the antenna cable to the female TNC antenna port labeled **ANT**.

Surge Protection

⚠WARNING
Atmospheric electrical charge accumulation can cause potential between the conductor and shield of the feed line, or cause lightning to strike an antenna. A lightning protector should be installed to prevent damage to equipment or injury to personnel.

The higher a radio antenna is mounted, the more likely the radio is to experience a surge event (e.g., a lightning strike). To protect the radio system from lightning damage, provide a path that allows the discharge of energy to bypass the radio system as well as a means of dissipating to ground any induced current pulses that are coupled into the radio system. A surge protector, such as the Radio Surge Protector With N Female Connectors (SEL part number 200-2004, shown in *Figure 2.4*), should be installed on the line and connected securely to a ground plate. In all surge protection applications, mount the surge protector at the building or enclosure entrance and ground the surge protector body. Ground the radio to the same point as the surge protector ground to avoid ground-rise potential damage.

For additional protection, you can use one or more in-line grounding cables (such as SEL part number 240-0124, shown in *Figure 2.5*) to provide a path to ground for any excess energy.

Figure 2.4 Radio Surge Protector With N Female Connectors (Part Number 200-2004)

Figure 2.5 In-Line Grounding Cable (Part Number 240-0124)

For detailed instructions regarding radio system lightning protection, see *AG2014-36: Radio System Lightning Protection Best Practices*, available at the SEL-FLR product webpage at selinc.com.

Ethernet Ports

Connect to the two rear-panel Ethernet ports (labeled **ETH 1** and **ETH 2**) using a standard RJ45 connector. Each of the rear-panel ports has a pair of LED indicators corresponding to the status of the port. This simplifies the detection of cabling errors when inserting and removing Ethernet cables from the rear of the device. *Figure 2.6* shows the location of these status LEDs and *Table 2.1* describes them. Enable **ETH 1** and **ETH 2** by using the web interface as shown in *Ethernet Network Interfaces* on page 4.15 (both ports are disabled by default).

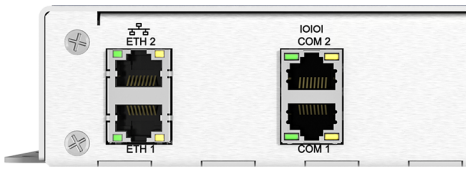


Figure 2.6 Rear-Panel Ethernet Port Link/Activity and 100 Mbps LEDs

Table 2.1 Ethernet Port LED Description

LED	Description
Green	Link/Activity
Yellow	100 Mbps

Serial Ports

Serial ports labeled **COM 1** and **COM 2** are not supported at this time.

Alarm Contact

The normally closed (NC) alarm contact terminals are labeled **01** and **02**. To provide remote alarm status indication, connect the alarm contact to your control system remote alarm input.

SEL-FLT Product Identification

To aid with product tracking and field deployment, each SEL-FLT is marked with a unique Device Address, as shown in *Figure 2.10*. The data packets transmitted by the SEL-FLT are identified by this device address. It is important to record the device address so you know which SEL-FLT device sent each data packet.

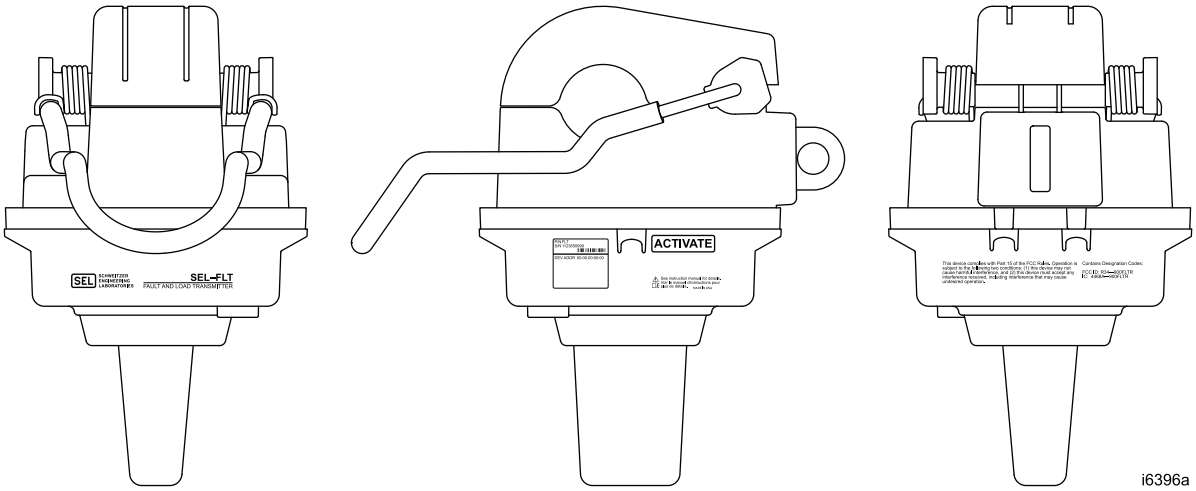


Figure 2.7 SEL-FLT Front, Side, and Rear Diagram

It is important to accurately record the location of each device during deployment to properly map device data points. Each device is provided with a tear-away adhesive identification label to record the installation location, as shown in *Figure 2.8*. Use these labels to record the device location during installation to update the description fields on the SEL-FLR web interface at a later time.

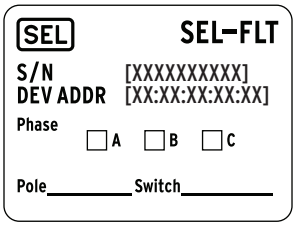


Figure 2.8 SEL-FLT Identification Label

SEL-FLT Wake-Up and Radio Activation

The SEL-FLT is shipped in a deep-sleep state to conserve power during storage. An SEL-FLR should be installed and operating within range of the SEL-FLT installation site *prior* to activating the SEL-FLT radio. If you activate an SEL-FLT before installing the SEL-FLR, the SEL-FLT will enter the back-off interval (see *Back-Off* on page 4.4 for details). Perform the following steps to wake up and enable the radio before deployment.

NOTE: Activate the SEL-FLT radio just prior to installation. Extended durations with the radio activated but without line current for power harvesting will deplete the rechargeable battery and then draw power from the non-rechargeable lithium battery.

Step 1. Remove the shorting bar from the CRSRTT magnet tool.

Step 2. Perform a long magnet press by holding the exposed magnet over the **ACTIVATE** label (see *Figure 2.9*) on the SEL-FLT for 10 seconds until a single yellow LED flashes rapidly. (A single red LED flashes first to indicate a short press, then the single yellow LED flashes to indicate the long press.)

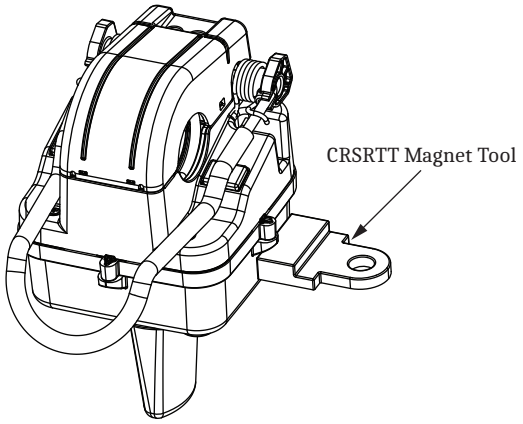


Figure 2.9 Activate the SEL-FLT

Step 3. Remove the magnet tool. The LEDs will flash in the Radio Activation display pattern to indicate the proper application of the magnet tool.

Step 4. Replace the shorting bar on the magnet tool for storage.

Step 5. The LEDs will flash in the Network Join display pattern after the radio joins with an SEL-FLR network. See *Getting Started* on page 2.21 for details on configuring the SEL-FLR.

The SEL-FLT device is now ready for installation.

SEL-FLT Installation

Installation Considerations

NOTE: Read and understand all instructions in their entirety before installing the SEL-FLT.

Install the SEL-FLT on overhead distribution conductors with a 6.4–38 mm (0.25–1.50 in) diameter. The SEL-FLT is rated for as high as 69 kV (line-to-line) and requires 5 A (default) or greater continuous load current to arm and reset the device.

⚠CAUTION
Do not attempt to slide the SEL-FLT along the conductor to move its position. To reposition the SEL-FLT, remove the sensor from the line and reinstall it at the correct location.

To ensure optimal SEL-FLT function, install the SEL-FLT with spacings according to *Figure 2.10*.

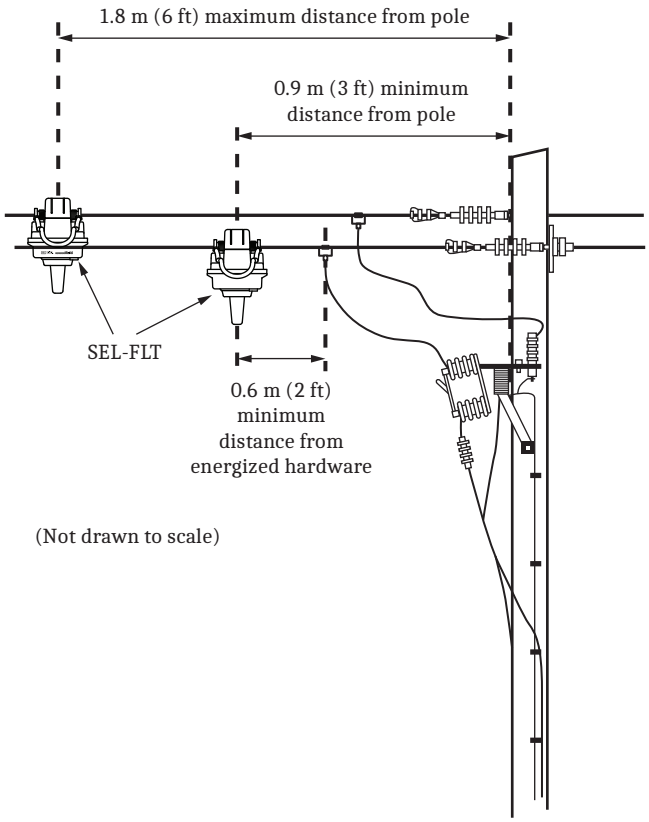


Figure 2.10 SEL-FLT Spacing Requirements

Installation

⚠DANGER
Always install fault indicators and sensors in accordance with normal safe operating procedures. These instructions are not intended to replace or supersede existing safety or operating requirements. Only trained qualified personnel with knowledge of high-voltage safety should install or operate fault indicators and sensors.

Step 1. Pull back on the hook eye to disengage the locking mechanism.

Step 2. Set the core prop (see *Figure 2.11*) to hold open the core. Any gap in the core mating surfaces will contribute to load data inaccuracy, so ensure that both core surfaces remain contaminant-free for the best product performance.

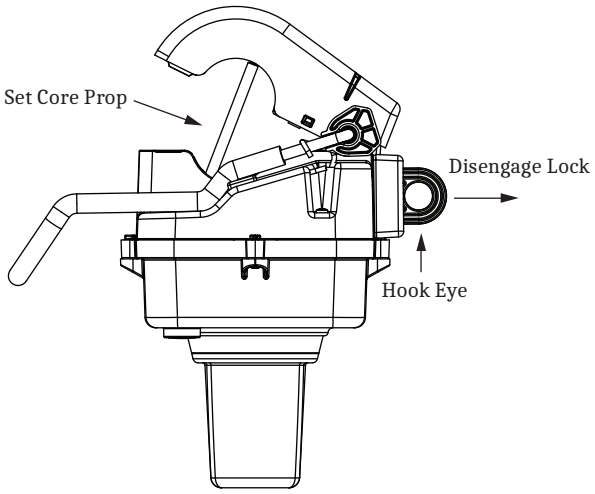


Figure 2.11 Set the Core Prop

Step 3. Grasp the hook eye with a shotgun-style hot stick.

Step 4. Position the SEL-FLT so that the end of its spring clamp fits behind the conductor.

Step 5. Apply force on the spring-loaded clamp by pulling downward on the SEL-FLT (see *Figure 2.12*).

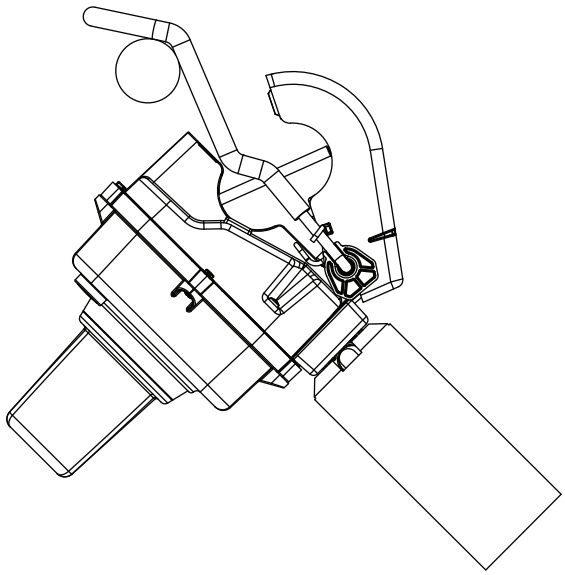


Figure 2.12 Install the SEL-FLT on the Conductor

Step 6. Slide the SEL-FLT onto the conductor until the core prop disengages and the core closes.

Step 7. Release the hot stick from the SEL-FLT hook eye. Releasing the hot stick locks the core.

Step 8. Position the unit so that the antenna points toward the ground (see *Figure 2.13*).

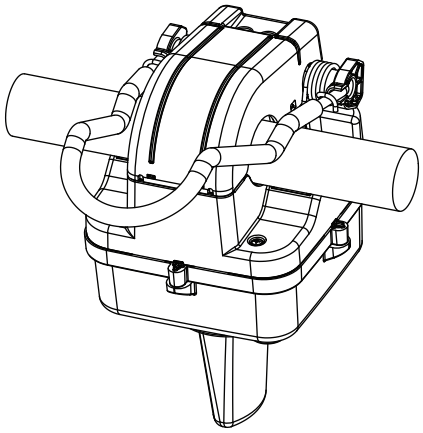


Figure 2.13 Position the Antenna Toward the Ground

Step 9. The LEDs will flash in the Armed display pattern after detecting greater than 5 A load current for 5 minutes (by default), indicating that the SEL-FLT is ready to detect fault events.

Step 10. The LEDs will flash the Network Join display pattern after the radio joins an SEL-FLR network.

Removal

Step 1. Use a hot stick to grasp the hook eye on the SEL-FLT (see *Figure 2.14*) and disengage the locking mechanism.

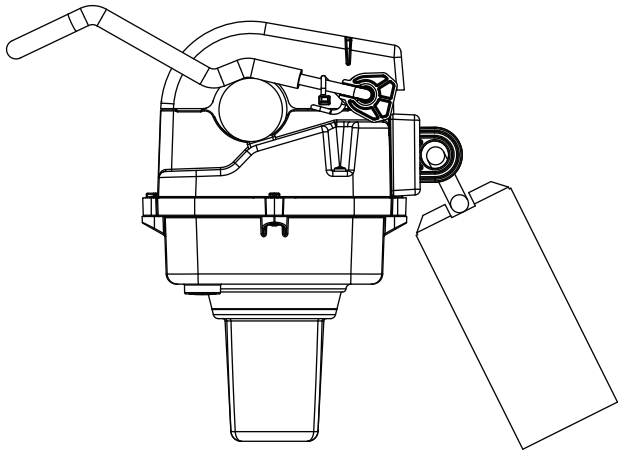


Figure 2.14 Disengage the Lock Mechanism

Step 2. Firmly pull downward on the hot stick (see *Figure 2.15*) to remove the SEL-FLT from the overhead conductor. After removing the SEL-FLT, turn off the radio by following the procedure in *Radio Deactivation* on page 2.15.

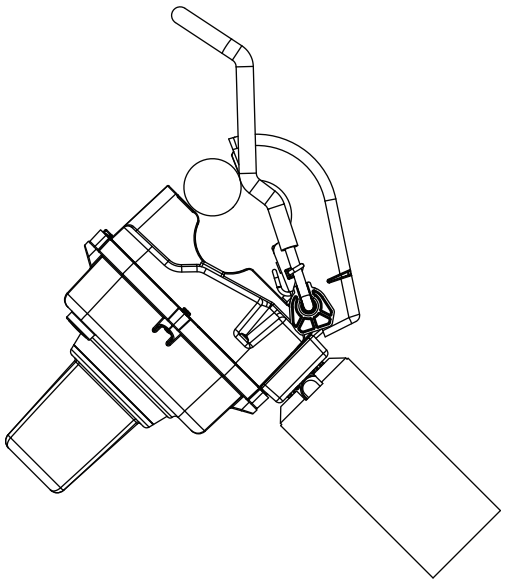


Figure 2.15 Remove the SEL-FLT From the Overhead Conductor

Radio Deactivation

Deactivate the radio after the product is removed to conserve power during storage.

Step 1. Remove the shorting bar from the CRSRTT magnet tool.

Step 2. Perform a long magnet press by holding the exposed magnet over the **ACTIVATE** label (see *Figure 2.9*) on the SEL-FLT for 10 seconds until a single yellow LED flashes rapidly. (A single red LED flashes first to indicate a short press, then the single yellow LED flashes to indicate the long press.)

Step 3. Remove the magnet tool. The LEDs will flash in the Radio Deactivation display pattern to indicate the proper application of the magnet tool.

Step 4. Replace the shorting bar on the magnet tool for storage.

Field Connections to the Enclosure

Connections to the SEL-FLR Enclosure

⚠CAUTION
Ground the SEL-FLR Enclosure before making and other connections to the enclosure.

The external connections on the SEL-FLR enclosure are located on the bottom of the enclosure. The connections provide a way to connect external antennas, ac power, and ground wire.

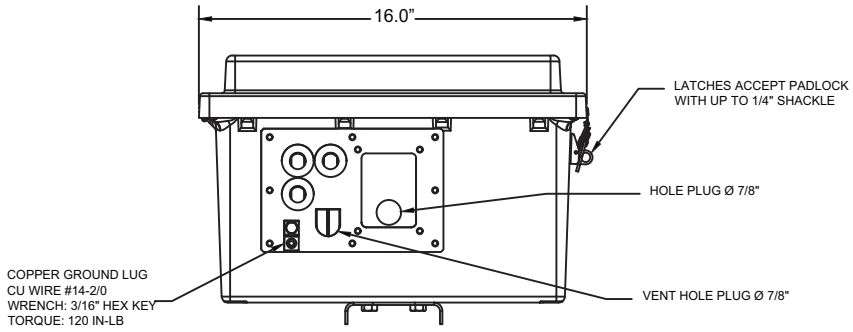


Figure 2.16 Bottom View of Enclosure With Connections

Installing the Enclosure

Overview

The following procedures describe the steps to install the SEL-FLR enclosure.

SEL-FLR Enclosure Grounding

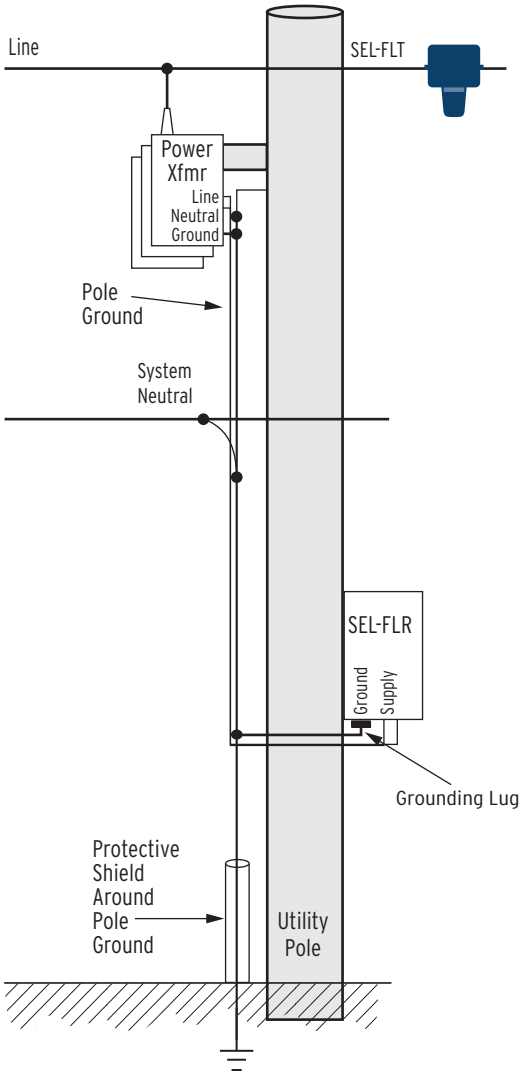


Figure 2.17 SEL-FLR Enclosure User Ground Connection to Required System Grounding

NOTE: All devices interfacing to the SEL-FLR enclosure must be connected to the same pole ground. *Figure 2.17* shows a suggested method of making these connections.

Step 1. Connect the pole ground to the grounding lug on the bottom of the SEL-FLR enclosure as shown in *Figure 2.17*.

The grounding lug accommodates No. 14–No. 4 conductors (solid or stranded). A protective shield around the pole ground is suggested to help prevent physical damage to the ground wire, such as preventing an open circuit.

NOTE: All connections to the SEL-FLR enclosure must be routed in close proximity to and parallel to their corresponding ground paths for adequate surge protection. The connections and their ground paths should be approximately equal in length. Use applicable IEEE and IEC grounding standards. Follow the proceeding recommendations to reduce high potentials from surges that can damage equipment.

Step 2. If using your own enclosure not provided by SEL, ensure that you ground all devices that interface with the SEL-FLR at the same pole.

In the SEL-FLR enclosure from SEL, the equipment included inside the enclosure (an SEL-FLR, power transformer, and communications equipment) comes prewired to the grounding lug. Devices on adjacent poles with their own pole ground (e.g., power transformer) must still connect to the pole ground for the SEL-FLR Enclosure.

Step 3. Route ac supply voltage (power) in parallel with the transformer ground path.

Step 4. When installing the SEL-FLR enclosure, include the following according to the manufacturers' recommendations:

- ➢ Protection of the power transformer with lightning arresters.
- ➢ Grounding of the power transformer tank.
- ➢ Grounding of the SEL-FLR enclosure.

GROUNDING INSIDE ENCLOSURE

As referenced in the accompanying steps, all grounding inside the enclosure should be brought to the 5/16-inch diameter bolt that protrudes through the floor of the enclosure. On the outside of the enclosure, this bolt is integral to the grounding lug shown in *Figure 2.17* and discussed in the first steps of this subsection (Control Grounding).

Battery Installation and Connection

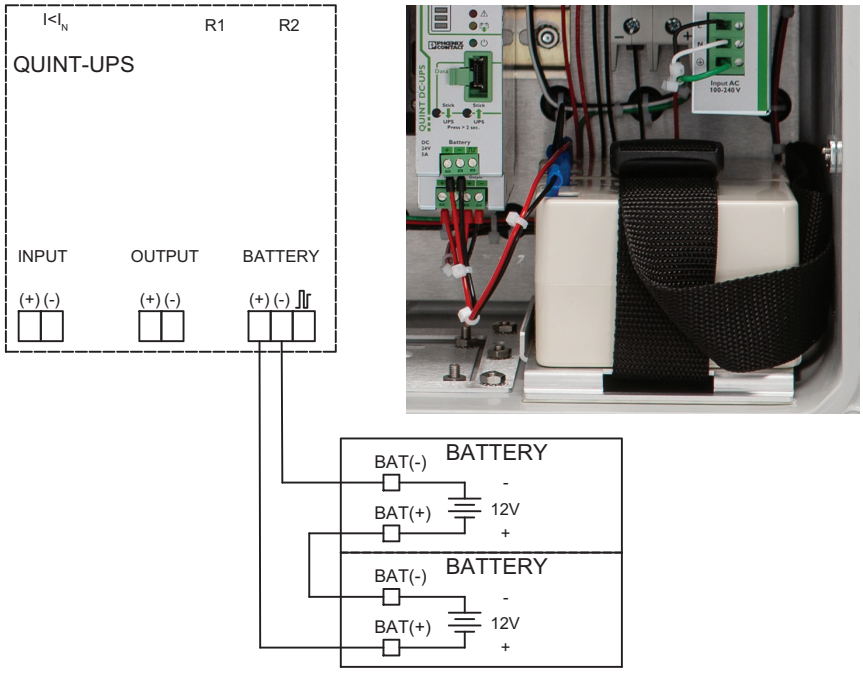


Figure 2.18 Battery Wiring Harness Connections and Battery Placement

Step 1. Follow any manufacturer installation recommendations and warnings for the battery.

Step 2. Inside the enclosure, unbuckle and move the two side-release buckle straps so that the raised battery platform is clear.

The straps should already be fitted underneath the slots provided on the raised platform, one strap oriented in one horizontal dimension and the other strap in the other horizontal dimension.

ENCLOSURE OPENINGS

No openings into the SEL-FLR Enclosure enclosure should be left uncovered, with the exception of the vented hole plugs provided by SEL. Any conduit or other wire entry must be properly sealed.

Step 3. Set the batteries beneath the disconnect switch and power supply on the raised platform in the bottom right corner of the enclosure with the terminals up and oriented toward the center of the enclosure as shown in figure *Figure 2.18*.

⚠WARNING
Do not transport the SEL-FLR Enclosure with the battery inside the enclosure.

Step 4. Ensure the small jumper wire in the harness connects the negative (–) terminal of one 12 Vdc battery to the positive (+) terminal of the other 12 Vdc battery to make an effective 24 Vdc battery.

Step 5. Fasten and secure the two side-release buckle straps over the battery, keeping the battery terminals clear.

Power Supply Connections

Two fused terminals are provided for 120 Vac power input. Connect the neutral wire to **FB2** and the hot wire to **FB1**. These connections are located opposite the pre-wired connections already terminated to the fuse block.

⚠WARNING
In the event a fuse is blown, ensure AC power is deenergized before gaining access to the fuse compartment in the fuse block. Ensure you find and address the cause of the blown fuse before refusing and reenergizing the enclosure.

Each fuse block contains a spare fuse. To gain access to the fuses, push upward on the fuse block tab until the assembly can swing outward.

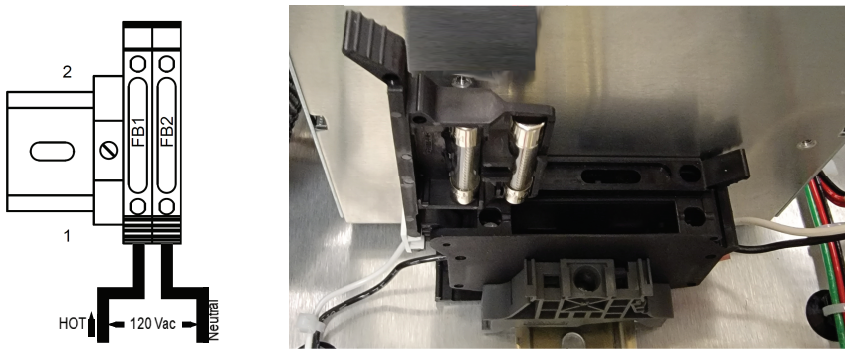


Figure 2.19 AC Power Input and Fuse Replacement

Pole Mounting the SEL-FLR Enclosure

The SEL-FLR enclosure comes with a factory-installed pole-mounting bracket. *Figure 2.20* and *Figure 2.21* show the front view of the enclosure.

Required equipment:

- (2x) 5/8" or 3/4" lag bolts
- 15/16" or 1-1/8" wrench
- Drill

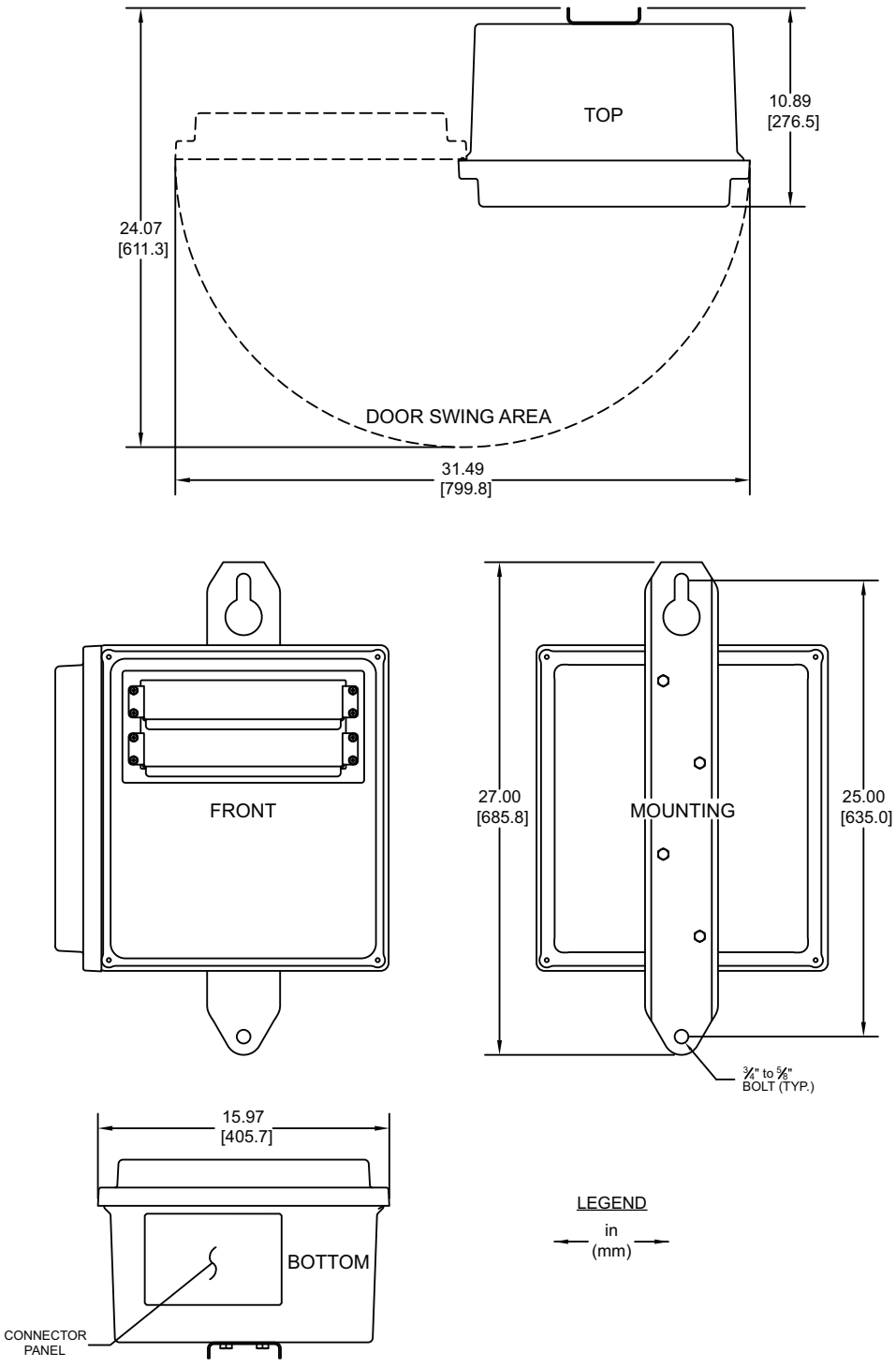


Figure 2.20 Enclosure Mounting Dimensions

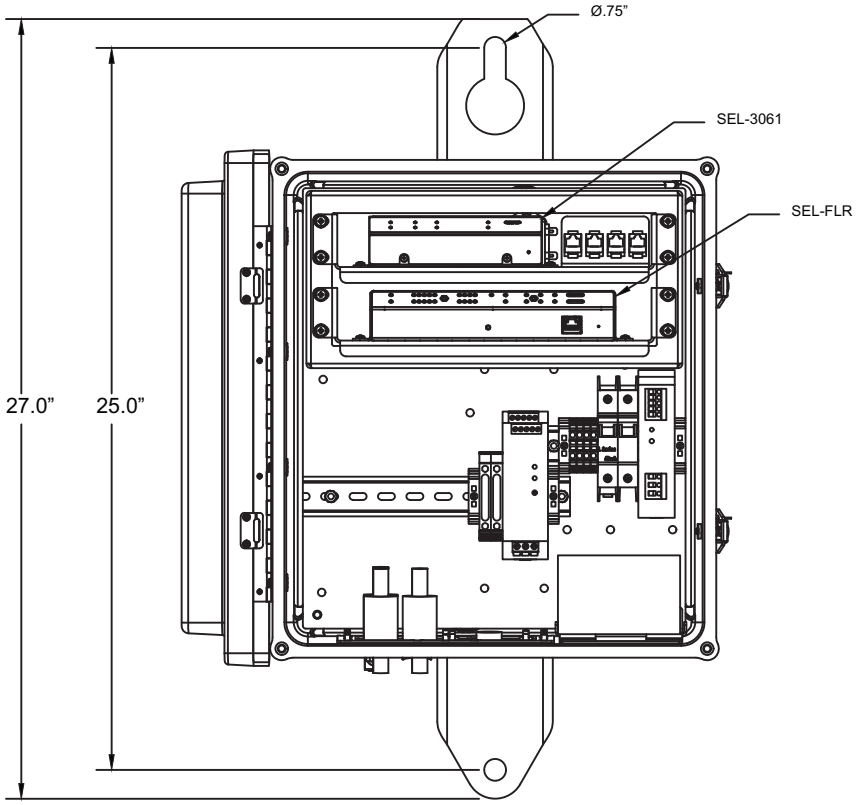


Figure 2.21 SEL-FLR Enclosure Interior

Step 1. Use the dimensions given in *Figure 2.20* or *Figure 2.21* and drill two pilot holes for the lag bolts.

Step 2. Install one lag bolt for the top mounting bracket.

Step 3. Hang the enclosure from the lag bolt.

Step 4. Install the other lag bolt into the bottom mounting bracket.

Step 5. Tighten both lag bolts.

Enclosure Maintenance

Visual changes may occur on fiberglass enclosures when they are exposed continually to environmental elements such as ultraviolet (UV) light, humidity, wind, and rain. Some of these changes are surface appearance changes, apparent color change (also called yellowing), and gloss loss. This happens because the ultraviolet light causes oxidation of the polyester resins used in the fiberglass enclosure, resulting initially in a powder like appearance and eventually in a snowflake like appearance on the outside of the enclosure. After a period of time, and under repeated exposure to these environmental elements, the reinforcing fibers may become exposed to the surface, resulting in a phenomenon called fiber bloom. Without any surface protection like wax and/or paint, this process can happen within the first two to five years, depending on the severity of the conditions. Fiber bloom is primarily an aesthetic condition. It should not affect the physical properties of the enclosure in an appreciable manner. Fiber bloom can also result in abrasions to personnel working with the enclosure.

Several factors affect the rate at which these changes progress on the enclosure:

- **Geographic Location.** Typically, an enclosure installed in tropical climates that sees high exposure to sun and humidity will see a more pronounced effect than other places. For example, an enclosure installed in Florida may see a more visible effect than an enclosure installed in Indiana.
- **Maintenance.** The type of protection applied and the time between repeated applications should be determined by the customer's personnel familiar with the local climate. Two types of protection are suggested here: painting and waxing. Painting offers better protection than waxing and, if properly applied, lasts longer than wax. Waxing is a simpler process than painting. However, it does not offer protection against ultraviolet light.

SEL recommends the following maintenance procedures to counteract the effects of fiber bloom.

1. **Painting.** Painting is a more involved process than waxing, but is known to provide effective resistance to fiber bloom. The following guides may be followed when painting the enclosures:
   - Rough up the surface by lightly rubbing with sandpaper.
   - Degrease the surface with an organic solvent such as alcohol or other domestic cleaning agent.
   - Wait for the surface to be clean and dry.
   - Apply the appropriate primer and top coat.

   Some general recommendations for paints are acrylic lacquer, a clear acrylic polyurethane, and Rust-Oleum universal formula spray paint.
2. **Waxing.** Waxing is recommended semi-annually, especially for areas that see significantly high exposure to the previously mentioned environmental elements. Any good commercially available wax like Carnauba paste wax can be used here. Note that although waxing provides protection against humidity, it offers almost no protection against ultraviolet light. Also, waxing is not meant to be a replacement for painting, but can be considered as a supplement to painting.

Note that appropriate personal protective equipment (PPE) such as glasses, a mask or gloves is recommended for the person doing the maintenance.

Getting Started

This section outlines the steps for commissioning the SEL-FLR and setting up the wireless network for communication with SEL-FLT devices.

This section includes the following:

Commissioning the SEL-FLR

The SEL-FLR includes an HTTPS web server for configuration and management functions.

For the initial connection to the SEL-FLR, the following will be required:

- A computer with a wired Ethernet port
- One RJ45 Ethernet cable
- The latest version of Google Chrome

Physical Network

NOTE: The SEL-FLR Ethernet ports do not allow incoming ping (echo requests) in firmware version R102-V0 and earlier.

Using a standard RJ45 Ethernet cable, connect the Ethernet port of your computer to the front-panel Ethernet port (**ETH F**) of the device.

Use Google Chrome to access the SEL-FLR user interface. The default URL for the web server via the **ETH F** port is https://192.168.1.2. See *Using Static IP Configuration* on page F.3 for how to configure the network configuration of a computer to a static IP address to connect to the SEL-FLR. Initially, the management interface can only be reached through the front Ethernet port. After commissioning (i.e., setting up a user account), additional management interfaces can be configured. See *Ethernet Network Interfaces* on page 4.15 for information on enabling an additional IP interface.

See *Section 4: SEL-FLR Configuration* for more information about the Captive Port feature. If the computer is configured to use static IP addresses, see *Appendix F: Configuring Windows Network Parameters* for assistance in configuring the network parameters of the computer.

NOTE: You may receive a certificate error from your browser. The message is dependent on the browser you are using. This error appears because the default certificate is a self-signed certificate and is not signed by a trusted Certificate Authority (CA). You will need to create a certificate exception to access the device login page. Your browser will provide instructions for doing this. For information on creating an X.509 certificate to eliminate this error, see *X.509 Certification Management* on page 5.17.

NOTE: The commissioning page only appears during the initial setup of a new unit or after a factory-default reset. After the device has been commissioned, the initial page will be the login page.

A new unit will have the front Ethernet port (**ETH F**) enabled and the Captive Port feature turned off.

Step 1. Open Google Chrome. In the address bar, enter https://192.168.1.2 to open the **Device Commissioning** page (as shown in *Figure 2.22*).

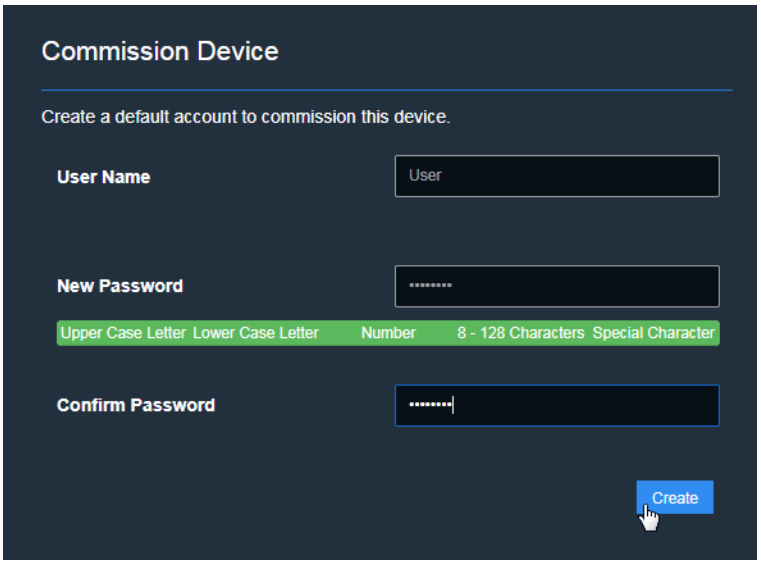


Figure 2.22 Device Commissioning Page

NOTE: In the event that the login credentials for all administrator and user manager accounts are lost, the device must be reset to its factory-default settings. For more information, see *Pinhole Reset* on page 5.19.

Step 2. Enter the account information for the first administrative user. This requires both a username and a password. You must type the password a second time (in the **Confirm Password** box) to confirm that it is entered correctly.

Step 3. Click **Submit** to complete commissioning. When the page reloads, log in as the administrative user to set up accounts and configure the system. After you successfully log in, the SEL-FLR redirects you to the Dashboard page.

Web Interface Overview

The SEL-FLR web interface provides a secure method by which to manage the SEL-FLT and SEL-FLR network. You must enter a valid username and password to access the web interface (see *User Accounts* on page 5.5).

Once logged in, you can view the status of the system on two dashboard views: one for the SEL-FLR (*Figure 2.23*) and the other for the SEL-FLT devices (*Figure 2.25*).

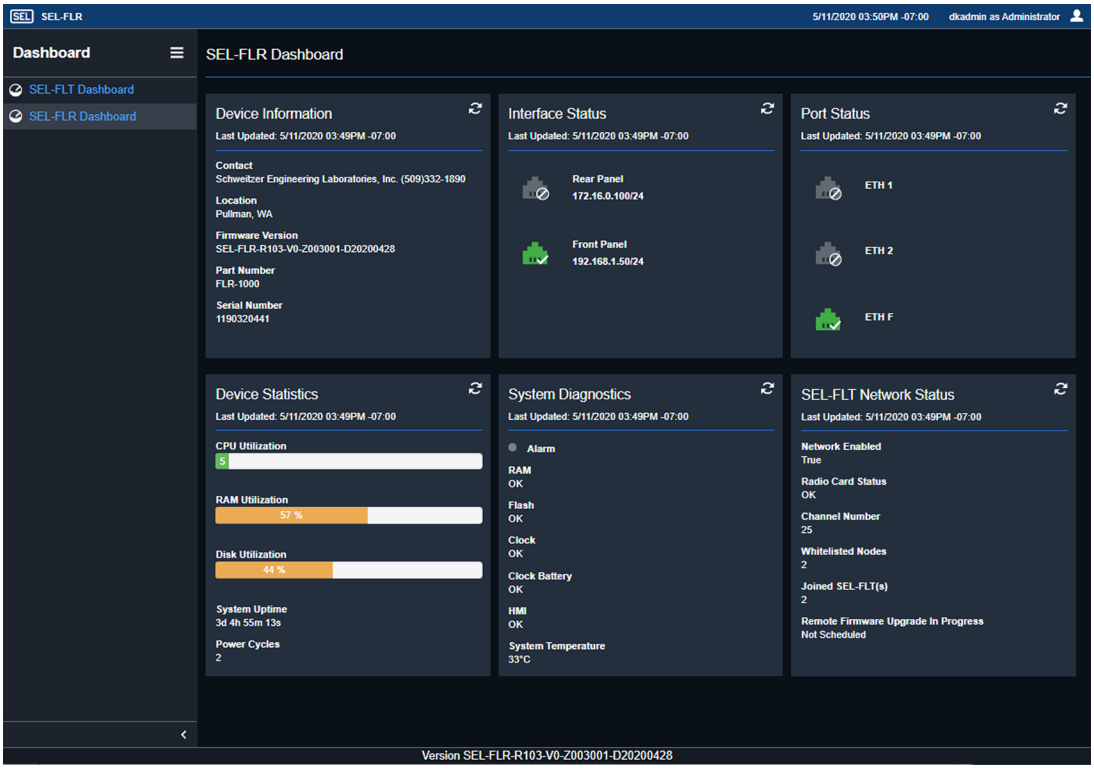


Figure 2.23 SEL-FLR Status View

The web interface allows you to configure and manage all aspects of the SEL-FLT and SEL-FLR network (with the correct account privileges). Use the drop-down menu shown in *Figure 2.24* to change the pages available in the left side panel. Click a page to navigate through the different SEL-FLR settings and status pages.

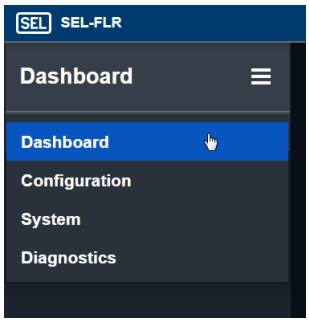


Figure 2.24 Web Interface Menu Navigation

Setting up Ethernet Ports ETH 1 and ETH 2

The IP Configuration and related parameters must be configured prior to connecting the rear-panel Ethernet ports to a network. See *Ethernet Network Interfaces* on page 4.15 for interface screens and network details.

Enabling the SEL-FLR Network Radio

NOTE: Choose different network frequencies in situations in which multiple SEL-FLT and SEL-FLR systems are installed in the same geographic area. If set to the same channel, the RF signals from devices on one network may interfere with the operation of devices on another network.

To configure Radio Frequency (RF) network communications for the SEL-FLT and SEL-FLR system, navigate to the **Configuration > Radio Network** page. Click **Enable Radio**, select a unique radio channel, and then click **Submit**. For help in determining a clear RF channel, the SEL-FLR web interface includes a channel analysis tool (see *Site Analysis* on page 4.8 for details).

The SEL-FLT devices do not require any RF settings. These devices scan all available radio channels while waiting to join a network.

Joining SEL-FLT Devices

The SEL-FLT and SEL-FLR system is an independent wireless network that must be configured prior to use. The SEL-FLR uses a whitelist to identify SEL-FLT devices that are allowed to join the network. When the SEL-FLR radio is initially turned on, it will populate a Discovery list with SEL-FLT devices that are not joined to any SEL-FLR device. SEL-FLT devices that appear on the Discovery list can be added to the whitelist, or devices can be manually entered into the whitelist. Once an SEL-FLT is on an SEL-FLR whitelist, the two devices establish a communications link and exchange security keys. After successfully exchanging security keys, the SEL-FLT is considered to be joined with the network.

Each SEL-FLT is uniquely identified by its Device Address (a unique 12-character identifier). Before configuring an SEL-FLR network, document the SEL-FLT Device Addresses to be included in the network, as well as additional information such as the feeder name, power system phase, and installation locations. The SEL-FLR keeps the Device Address and additional data fields in the SEL-FLT Whitelist page to simplify network management. See *SEL-FLT Sensor Management* on page 4.12 for example lists.

Ensure the SEL-FLT Joins the Correct Network

Each SEL-FLT can only be joined with one SEL-FLR network. If the SEL-FLT is accidentally entered in the whitelist for two SEL-FLR systems, the join will be made with the first SEL-FLR that successfully exchanges security keys.

Once joined, an SEL-FLT will remain on a network as long as the SEL-FLR is active and the SEL-FLT devices remain on the whitelist. If for some reason the SEL-FLR is no longer operating (e.g., the power source is removed), or the wireless signals are not reaching a set of SEL-FLT devices because of the radio path interference, the joined SEL-FLT devices will time out and become unjoined. If the Device Addresses of these SEL-FLT devices are present on the whitelist of another in-range SEL-FLR, the devices will exchange security keys with the new SEL-FLR and join to that new network.

For an overview of the encrypted key exchange, see *Appendix E: X.509*.

SEL-FLR Front-Panel LEDs

The SEL-FLR front panel is equipped with an **ENABLED** LED to indicate the state of the device.

Table 2.2 SEL-FLR Front-Panel ENABLED LED

Label	Color	Description
ENABLED	Green	Device is on and has passed self-tests.
	Off	Device is off or has failed self-tests.

Refer to *Section 9: Maintenance, Testing, and Troubleshooting* for information on SEL-FLR self-test functions.

System Dashboard Overview

The web interface includes two dashboards with information relating to device hardware, operational status, network statistics, and sensor data. The SEL-FLR Dashboard page (shown in *Figure 2.23*) shows the status, statistics, and diagnostic information pertaining to the SEL-FLR, communications ports, and radio network status. The SEL-FLT Dashboard page (shown in *Figure 2.25*) shows the status, statistics, and diagnostic information for each of the SEL-FLT devices on the network. System parameters cannot be changed from the dashboard view.

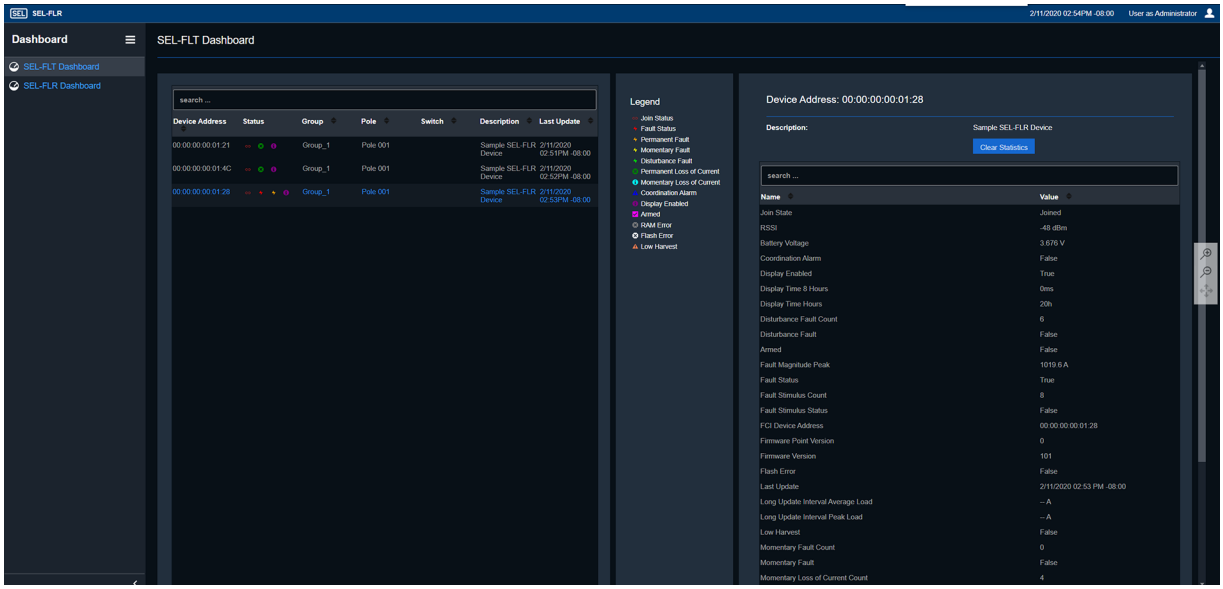


Figure 2.25 SEL-FLT Dashboard

The status of each device on the SEL-FLT Dashboard page is represented by the symbols shown in *Figure 2.26*. *Table 2.3* defines the different statuses that can be shown for each SEL-FLT device.

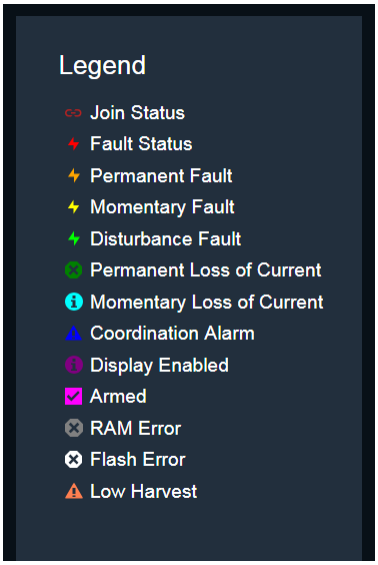


Figure 2.26 SEL-FLT Dashboard Legend

Table 2.3 SEL-FLT Device Status Descriptions

Label	Description
Join Status	The SEL-FLT device is joined to the SEL-FLR.
Fault Status	The SEL-FLT has detected a fault stimulus event.
Permanent Fault	The SEL-FLT has detected a permanent fault event.
Momentary Fault	The SEL-FLT has detected a momentary fault event.
Disturbance	The SEL-FLT has detected a disturbance event.
Permanent Loss of Current	The SEL-FLT has detected a permanent loss-of-current event.
Momentary Loss of Current	The SEL-FLT has detected a momentary loss-of-current event.
Coordination Alarm	The SEL-FLT has detected a coordination alarm.
Display Enabled	The SEL-FLT local LED display is enabled.
Armed	The SEL-FLT is armed.
RAM Error	The SEL-FLT has detected a RAM error.
Flash Error	The SEL-FLT has detected a flash error.
Low Harvest	The SEL-FLT has insufficient power harvesting.

SECTION 3

Applications

Overview

The SEL-FLT Fault and Load Transmitter improves overall system reliability through accurate monitoring of the distribution grid. The SEL-FLR manages and aggregates data from multiple SEL-FLT devices in the immediate vicinity in order to provide load monitoring and fault reporting to SCADA operators. The flexibility of this system allows it to be applied at several locations throughout the distribution system to increase overall system visibility and reliability.

Send line crews directly to areas in need of restoration, thus reducing outage times. The system enables faster fault location and highly accurate load monitoring by aggregating details from the distribution grid.

This section includes the following:

SEL-FLT Applications

Event Detection

The SEL-FLT detects a variety of system events, such as permanent faults and temporary outages. Fault detection alone greatly reduces the time it takes to locate a fault, which improves reliability metrics such as Customer Average Interruption Duration Index (CAIDI) and System Average Interruption Duration Index (SAIDI). In addition to fault detection, the SEL-FLT also discerns between permanent and momentary faults and detects system outages. The SEL-FLT implements advanced algorithms to provide accurate detection and distinction of all event types. You can focus on specific system events by filtering message types through the settings. Additional information provided by the SEL-FLT, such as device status and event statistics, improves awareness of system conditions, and maximizes the effectiveness of the SEL-FLT. By identifying high-risk trouble areas on the system, you can take corrective action before a fault occurs.

Load Monitoring

The SEL-FLT monitors load current and reports the 24-hour peak, 24-hour average, 5-minute peak, and 5-minute average. Use the load monitoring feature to enhance switching decisions for daily feeder load management and load reconfiguration. Highly accurate SEL-FLT load information helps you locate sources of unbalanced phases and optimize circuit reconfiguration for balanced conditions, and also aid in the detection of sources of power theft. The SEL-FLR

aggregates and displays all of the SEL-FLT load data. The load information can also be sent from the SEL-FLR to a SCADA system or an outage management system (OMS) via DNP3.

Long Feeders

Improve management of long remote feeders with the SEL-FLT by dividing feeders into smaller sections to increase the resolution of the fault location and load current points. The SEL-FLT economically brings visibility to remote feeders that typically take hours to patrol. The line powering capability expand applications to almost anywhere on an overhead distribution system. Apply sets of SEL-FLT devices on long feeders to quickly divide the circuit into smaller sections to provide more precise fault resolution.

Taps and Branches

Distribution systems often have one or more complex feeders that split into many different directions to service customers. Install SEL-FLT devices immediately downstream of a tap or branch to provide visibility of which tap the fault is on. Quick identification of a faulted tap will increase response times, even in complex circuits with many taps or laterals.

Dips and Risers

Dips (overhead-to-underground transitions) and risers (underground-to-overhead transitions) naturally segment the circuit and serve as an ideal location to apply SEL-FLT. Place the SEL-FLT on overhead sections at these transition points provide visibility of downstream faults.

System Applications

System-Wide Reliability Improvements

The SEL-FLT supports overhead fault and load monitoring applications across the entire distribution system (to as high as 69 kV). Multiple SEL-FLT devices send fault and load data to a single SEL-FLR within line of sight. The SEL-FLR connects to the SCADA system via a preferred backhaul channel (e.g., radio, Ethernet, cellular, fiber). *Figure 3.1* shows a basic system overview that establishes a system-wide coverage of the distribution circuit by placing SEL-FLR enclosures and SEL-FLT units at strategic locations throughout the system. Strategic placement of SEL-FLT devices provides a means for improving reliability indices such as CAIDI and Momentary Average Interruption Frequency Index (MAIFI). Through early identification of a momentary fault, the cause of the fault can be addressed to eliminate its future impact on MAIFI.

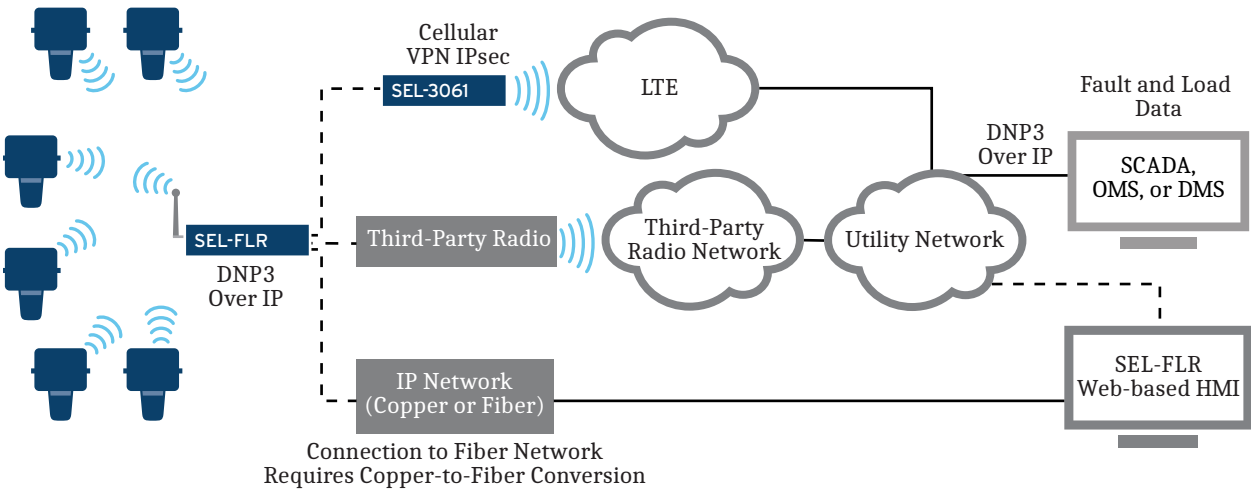


Figure 3.1 SEL-FLT/SEL-FLR System Overview

Load Reconfiguration and Management

The SEL-FLT provides loading information as frequently as every 5 minutes. Load information helps with daily distribution circuit planning activities such as load reconfiguration and management. During an outage, system operators may attempt to sectionalize the distribution circuit to restore power to as many customers as possible.

Accurate circuit loading at taps and branches enables operators to precisely add customers to an energized feeder not affected by the outage to improve CAIDI. The accurate SEL-FLT load data enhance circuit load flow models to improve estimates, minimize equipment stress, reduce the chances of overloading a feeder, and help you restore power to more customers.

The traditional method for locating unbalanced phases is a very time-consuming process. To identify unbalanced phases, crews must manually apply ammeters to power lines and record the current value of each phase throughout the distribution system. The SEL-FLT automates this process by providing periodic load data to a remote SCADA system. The SEL-FLT load data provide engineers with insight into the exact load levels throughout the distribution circuit. By using the SEL-FLT load data, circuit reconfiguration can be optimized to achieve a more balanced system.

Difficult-to-Access Circuits

Overhead circuits often run through difficult-to-access areas that pose unique hazards, such as forests, rocky terrain, or restricted sites. Deploying SEL-FLT devices in these areas provides remote indication of faults, fault types, and load data.

Communication between the SEL-FLT and an SEL-FLR eliminates the need to patrol the line for visual fault indications. In addition, you can enable Momentary Fault messages to narrow down faults that are caused by tree branches contacting the power line, which helps improve reliability metrics such as MAIFI.

Remote Status on Distribution Equipment

The SEL-FLT provides a remote status of non-SCADA enabled distribution equipment (breakers, reclosers, switches, etc.) Place an SEL-FLT immediately downstream of non-communicating substation breakers to remotely identify which breaker has operated. Install SEL-FLT devices upstream and downstream of a switch, disconnect, or recloser to monitor the status (open or closed) of the equipment.

Distribution Circuit Planning

Utility planning groups need to understand load growth and load trends throughout a distribution system. Accurate load reports from the SEL-FLT help determine if equipment ratings are sufficient or running near capacity. The SEL-FLT loading reports allow you to project areas of load increase, determine areas of system stress, and better plan for equipment upgrades throughout the system.

Power Theft Detection

AMI-enabled meters and traditional analog meters provide power usage data at the loads where they are installed, but they do not measure load upstream of their location. Therefore, undetected power theft is possible between the meter and the source.

One common example of power theft occurs when someone taps into low-voltage power cables to feed unmetered loads. In many cases, a central meter at the transformer can identify whether theft is occurring in a general area. Because of the vast amount of low-voltage cables exiting some transformers, it is difficult to specifically locate the unmetered loads. By installing the SEL-FLT on low-voltage cables immediately exiting the transformer, you can determine on which cables the unmetered loads are located, as shown in *Figure 3.2*.

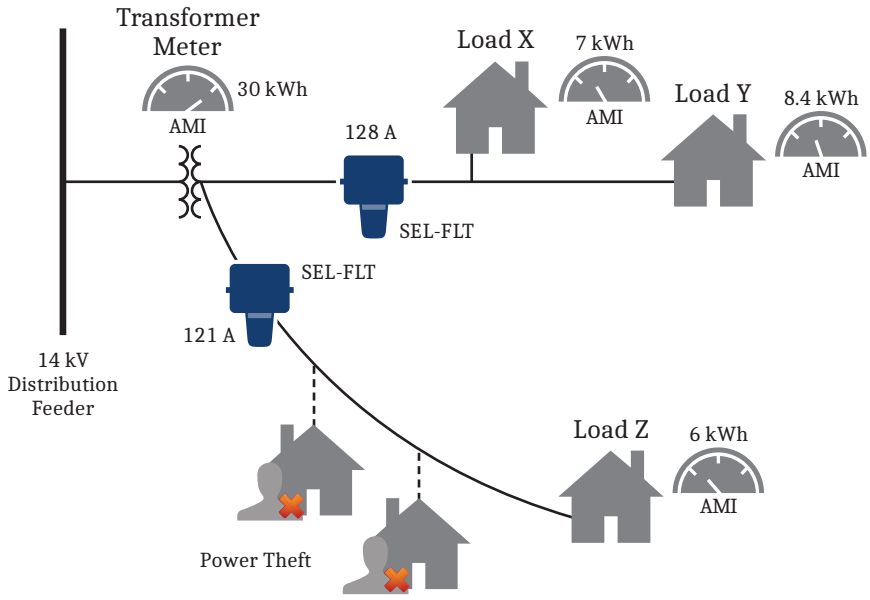


Figure 3.2 Determining Power Theft

In the example shown in *Figure 3.2*, Loads X and Y match the load current reported by the upstream SEL-FLT. However, the SEL-FLT monitoring Load Z reports a much higher load than the meter at Load Z. Therefore, the power theft must be occurring somewhere on the branch that feeds Load Z.

SECTION 4

SEL-FLR Configuration

Overview

This section provides information on the wireless network behavior and protocol, including information about the following:

Radio Network

The 900 MHz radio link between the SEL-FLR and SEL-FLT devices is optimized for transmitting sensor data. This section describes the radio network overview, topology, security, radio links, and channel selection.

This section includes the following:

Radio Network Overview

NOTE: SEL-FLR networks use a star configuration and do not support the use of repeaters.

NOTE: The SEL-FLT will detect fault events and flash local LED display patterns even when it is not connected to an SEL-FLR network.

The SEL-FLT and SEL-FLR both integrate a low-power radio that operates in the license-free 900 MHz industrial, scientific, and medical (ISM) band. The wireless network operates as a star topology with multiple end devices (SEL-FLT) talking to a single collector (an SEL-FLR), as shown in *Figure 4.1*.

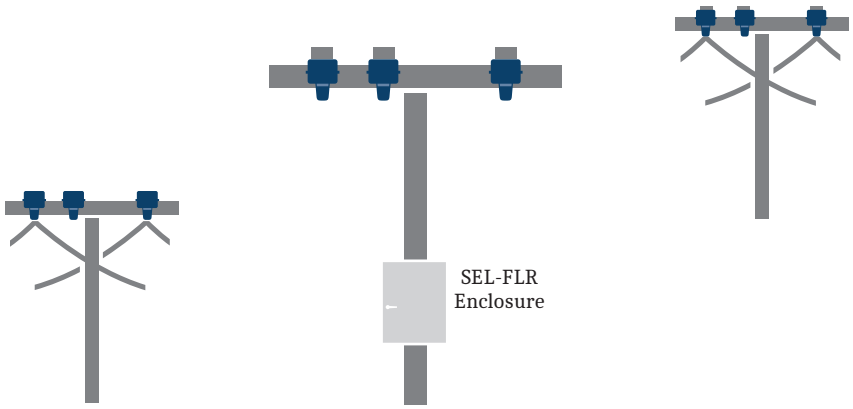


Figure 4.1 Node Radio Network With Star Topology

The SEL-FLT communicates with the SEL-FLR collector via a purpose-built protocol for line sensor applications. The SEL-FLT and SEL-FLR network implements a poll-response protocol optimized for sensor applications. The SEL-FLR sends poll messages to all connected SEL-FLT devices, and each SEL-FLT responds to these poll messages with either a network heartbeat message or a data message. All network heartbeat and data messages sent by the SEL-FLT are then acknowledged by the SEL-FLR.

Each group of collocated SEL-FLT devices will have an operating range, or maximum communication distance, that is determined by the system and the environment (see *Appendix D: Link Budget Analysis* for more information). The links require a clear line of sight, and link quality can be affected by geography, obstructions, SEL-FLR antenna selection and placement, and the amount of 900 MHz background traffic or noise. For best results, install SEL-FLT devices at locations where they can be seen from the SEL-FLR antenna to confirm there are no obstructions to the line of sight. See *Section 2: Installation* for full details on network deployment.

Encryption and Security

The radio communications protocol ensures confidentiality and integrity of data between SEL-FLT and SEL-FLR devices. The protocol also ensures that all devices on the network are trusted by authenticating devices through the use of simple public-key infrastructure (SPKI) cryptography. See *Simple Public-Key Infrastructure* on page E.5 for more information.

During the initial joining process, the SEL-FLT and SEL-FLR digitally sign messages. The use of distinct digital signatures provides authentication of the SEL-FLT and SEL-FLR devices and ensures that all devices joining the network are SEL-certified. See *Digital Signatures* on page E.3 for more information.

Once an SEL-FLT and SEL-FLR have established trust by verifying digital signatures, they use a modified ZigBee symmetric-key key exchange (SKKE) for key exchange. The SEL-FLT and SEL-FLR use a shared Product Master key to establish a unique Session key. Once the key exchange is complete, the SEL-FLT and SEL-FLR are joined.

Only authenticated SEL-FLT devices that are whitelisted by an SEL-FLR are allowed to join its network. After an SEL-FLT is joined with an SEL-FLR network, all message exchanges use AES 128-bit encryption and CCM authentication. If the link between the SEL-FLR and an SEL-FLT device is interrupted, the devices will need to rejoin with one another and establish new Session keys.

Key Management

Product Master Key (256 Bits)

The Product Master key is preshared by all SEL-FLT and SEL-FLR devices. It provides a cryptographic authentication mechanism for rejecting session requests by unauthorized devices.

Session Key (128 Bits)

Session keys are used to encrypt and authenticate all protected user data during transmission. They are generated when an SEL-FLT joins an SEL-FLR network, and each Session key is unique to that link. Session keys are generated by the process outlined in FIPS 98, which uses the Product Master key as the hash key, as well as session challenges and unique identifiers from the SEL-FLR and the joining SEL-FLT. The session challenges are produced using an integrated physical random number generator (RNG). The key exchange uses the SKKE protocol. Only the challenges and unique identifiers are sent over-the-air. The use of unique session keys and unique initialization vectors limits the amount of data that is encrypted with a single key value and prevents replay attacks, thus strengthening the system against cryptanalytical attack.

Encryption Algorithm

The SEL-FLT and SEL-FLR system implements the Advanced Encryption Standard (AES) algorithm with a key length of 128 bits. This algorithm is a secure means of encrypting data and provides proven resistance to modern cryptanalysis.

The AES encryption function provides cryptographically strong data confidentiality by using a 128-bit secret key to scramble the contents of each frame prior to transmission. The output of the encryption process is a function of both the message and a Session key, as shown in *Figure 4.2*.

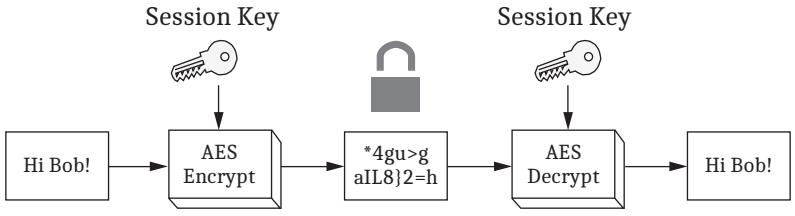


Figure 4.2 Operation of the AES Encryption Function

This encryption process must be completely reversible by an authorized individual with access to the secret decryption Session key. Authority to read a message is only granted by sharing the knowledge of the secret decryption Session key. Ideally, only individuals with knowledge of the decryption Session key can reverse the encryption operation and interpret the protected message. The AES encryption algorithm used in the SEL-FLT and SEL-FLR system is a symmetric block cipher with a 128-bit encryption/decryption Session key.

Establishing Communications Links

The SEL-FLT radio must be activated before the SEL-FLT can join a network (see *SEL-FLT Wake-Up and Radio Activation* on page 2.10 for details). *Figure 4.3* represents a typical joining process for the SEL-FLT and SEL-FLR.

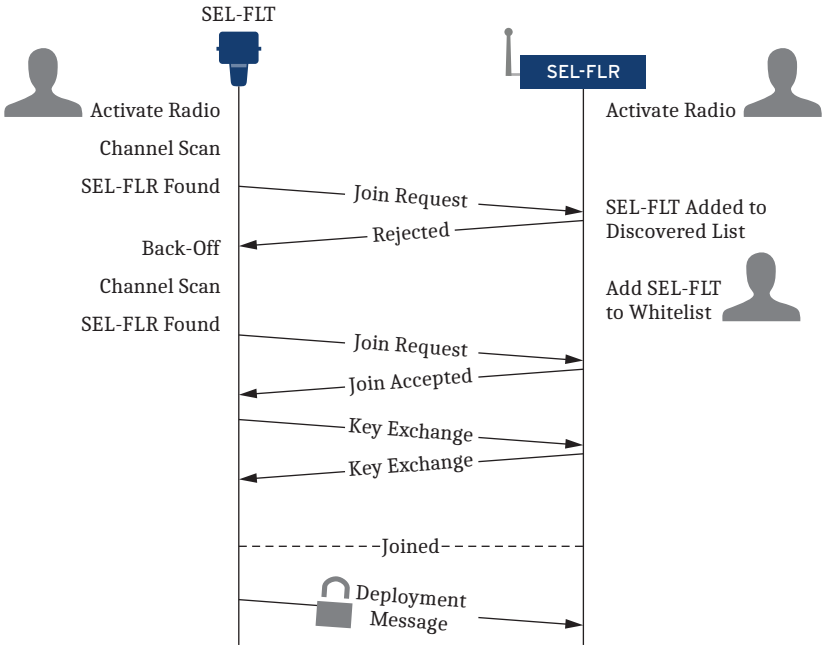


Figure 4.3 Joining Process

After the radio is activated, the SEL-FLT begins scanning all channels looking for an SEL-FLR network with which to join. The SEL-FLT will identify itself to any SEL-FLR found during this scan as being unjoined. Once the SEL-FLT makes contact with an SEL-FLR, the SEL-FLR will add the SEL-FLT device to its Discovery list. The SEL-FLR will then consult its whitelist to determine whether that SEL-FLT is allowed to join its network (see *SEL-FLT Sensor Management* on page 4.12 for details). If an SEL-FLT is initially unsuccessful in joining an SEL-FLR network, it continues to scan each subsequent frequency channel, but at a reduced interval dictated by its back-off feature.

When the SEL-FLT finds a network that it is allowed to join, it will establish security Session keys and exchange network settings. The SEL-FLT will typically join an SEL-FLR network within 5–10 minutes, with a maximum joining time of 75 minutes. If the SEL-FLT has not joined a network within 75 minutes, see *Section 9: Maintenance, Testing, and Troubleshooting* for help or contact SEL.

After joining a network, the SEL-FLT sends a Deployment message and flashes the local LEDs in the Network Join display pattern to indicate a successful network link.

Back-Off

Continuous channel scanning when no SEL-FLR is active within range of an SEL-FLT can rapidly deplete the power available to the SEL-FLT. If the SEL-FLT is unsuccessful at joining an SEL-FLR network, it will continue scanning channels after a delay. This is referred to as back-off. To conserve power after a failed attempt to join a network, the SEL-FLT will enter a back-off state for 15 minutes. While in a back-off state, the SEL-FLT will neither scan channels looking for an SEL-FLR nor join any networks. After the 15 minute back-off period, the SEL-FLT will resume scanning channels for an SEL-FLR network to join. The SEL-FLT will continue to enter a back-off state for 15 minutes between unsuccessful join attempts.

Lost Link

An SEL-FLT may become unjoined from an SEL-FLR for various reasons, including poor network coverage, RF interference, or an SEL-FLR restart.

Once an SEL-FLT has joined an SEL-FLR network, both the SEL-FLT and the SEL-FLR monitor communication with one another for continued link activity. The SEL-FLT monitors SEL-FLR poll messages and heartbeat acknowledgments to verify that the SEL-FLR is still active on the network. The SEL-FLR monitors the SEL-FLT heartbeat message to verify that the SEL-FLT is still active on the network. If the SEL-FLR does not receive a network heartbeat message from a specific SEL-FLT for 15 minutes, then that link is considered lost. *Figure 4.4* shows an example of the lost link process, and *Figure 4.5* shows an example of a lost link status on the SEL-FLT Dashboard page in the web interface. When an SEL-FLR determines that a previously active SEL-FLT on the network has been lost, it initiates a connect poll to allow that SEL-FLT to rejoin the network.

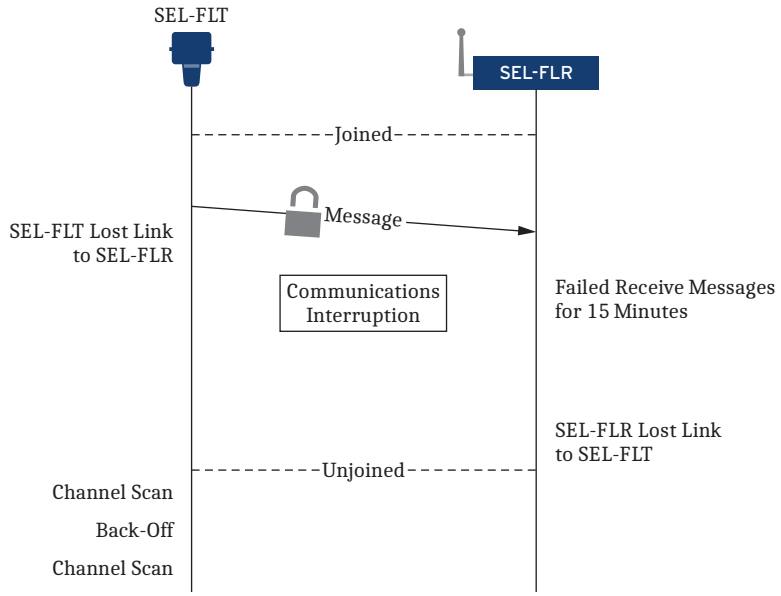


Figure 4.4 Lost Link Process

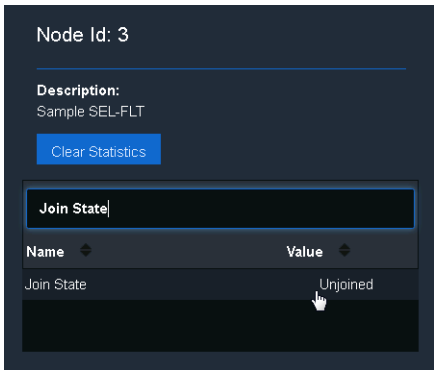


Figure 4.5 Lost Link Status

If the SEL-FLT does not receive any polls, or it does not receive a heartbeat acknowledgment after 90 seconds, it assumes it has lost communication with the previous SEL-FLR network. The SEL-FLT will start a channel scan to find a new

join request, and then enter the back-off sequence if it cannot join a network. This mutual link activity monitoring prompts both the SEL-FLR and SEL-FLT to initiate the appropriate actions to allow lost SEL-FLT devices to rejoin the network.

SEL-FLR Power Cycle

In situations where the SEL-FLR briefly loses power or the user initiates a device reset, all SEL-FLT devices will become unjoined and enter the back-off sequence described in *Back-Off* on page 4.4. All SEL-FLT devices will rejoin the network after the SEL-FLR restarts (see *Establishing Communications Links* on page 4.3). SEL-FLT devices may not attempt to join the SEL-FLR network for as long as 15 minutes due to the back-off sequence.

SEL-FLR Radio Network Settings

The SEL-FLR radio is initially disabled, and it must be enabled to establish a radio network. The initially disabled state allows the SEL-FLR to be turned on without interfering with any nearby equipment. Turn the radio on by navigating to the **Configuration > Radio Network** page in the user interface, as shown in *Figure 4.6*, and clicking **Submit**.

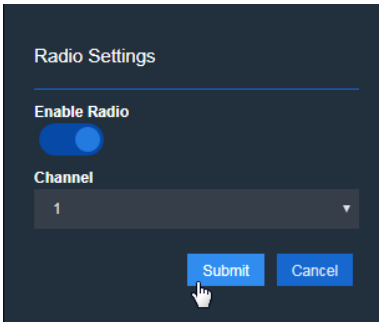


Figure 4.6 Radio Network Settings

Table 4.1 shows the radio enable and channel selections that appear on the Radio Network page.

Table 4.1 SEL-FLR Radio Settings

Setting Name	Value	Default	Description
Enable Radio	ON, OFF	OFF	Enables the SEL-FLR radio, which allows the SEL-FLR to begin establishing links to SEL-FLT devices that are included in its whitelist.
Channel	1–25 (FLR-1000) 1–11 (FLR-1003) 1–16 (FLR-1006) 1–6 (FLR-1007) 1–25 (FLR-1008) 1–12 (FLR-1009)	1	Selects the channel for operation of the SEL-FLR wireless network.

Channel Selection

NOTE: Configure adjacent SEL-FLR networks to use different radio channels to minimize interference.

All devices joined with the same network will communicate on the same channel. The channel is also set by going to the **Configuration > Radio Network** page, as shown in *Figure 4.6*. Setting the SEL-FLR channel will configure the channel for the entire network. SEL-FLT devices do not have a channel selection setting because they automatically learn the channel from the SEL-FLR with which they join.

When there are two or more SEL-FLR devices within range of an SEL-FLT performing a channel scan, the SEL-FLT will identify itself to the SEL-FLR operating on the network that it finds first (typically the lowest-frequency channel). If it is allowed to join that network, it will do so and stop scanning channels. If it is not allowed to join that network, it will continue to scan channels at the next highest frequency channel and will identify itself to the next SEL-FLR network that it encounters.

For best performance when two or more SEL-FLR radio networks are deployed with overlapping coverage areas, allow for a 2 MHz separation between each SEL-FLR network. For example, consider two SEL-FLR devices installed in close proximity to one another. If one of those is operating at 919 MHz, do not select a channel in the 917–921 MHz range on the other SEL-FLR.

The SEL-FLR network operates on a selectable frequency corresponding to one of the channel assignments shown in *Table 4.2*.

Table 4.2 SEL-FLR Channel Mapping by Model/Country

Frequency (MHz)	Channels					
	FLR-1000 FLT-1000 (U.S.A., Canada, Mexico)	FLR-1003 FLT-1003 (Peru)	FLR-1006 FLT-1006 (Brazil)	FLR-1007 FLT-1007 (Costa Rica)	FLR-1008 FLT-1008 (Argentina)	FLR-1009 FLT-1009 (Ecuador)
903	1		1		1	
904	2		2		2	
905	3		3		3	
906	4		4		4	
907	5				5	
908	6				6	
909	7				7	
910	8				8	
911	9				9	
912	10				10	
913	11				11	
914	12				12	
915	13				13	
916	14		5		14	1
917	15	1	6		15	2
918	16	2	7		16	3
919	17	3	8		17	4
920	18	4	9		18	5
921	19	5	10		19	6
922	20	6	11	1	20	7
923	21	7	12	2	21	8
924	22	8	13	3	22	9
925	23	9	14	4	23	10
926	24	10	15	5	24	11
927	25	11	16	6	25	12

Site Analysis

NOTE: The Site Analysis feature is only available when the radio network is disabled.

The SEL-FLR features a site analysis tool to aid in selecting an RF channel that is free of any unidentified radio activity. Navigate to the **Configuration > Radio Network** page and click **Scan** to measure the average and peak power on each of the available radio channels. The resulting table represents the relative radio power at the SEL-FLR antenna input. An example scan is shown in *Figure 4.7*. This procedure takes approximately 10 seconds.

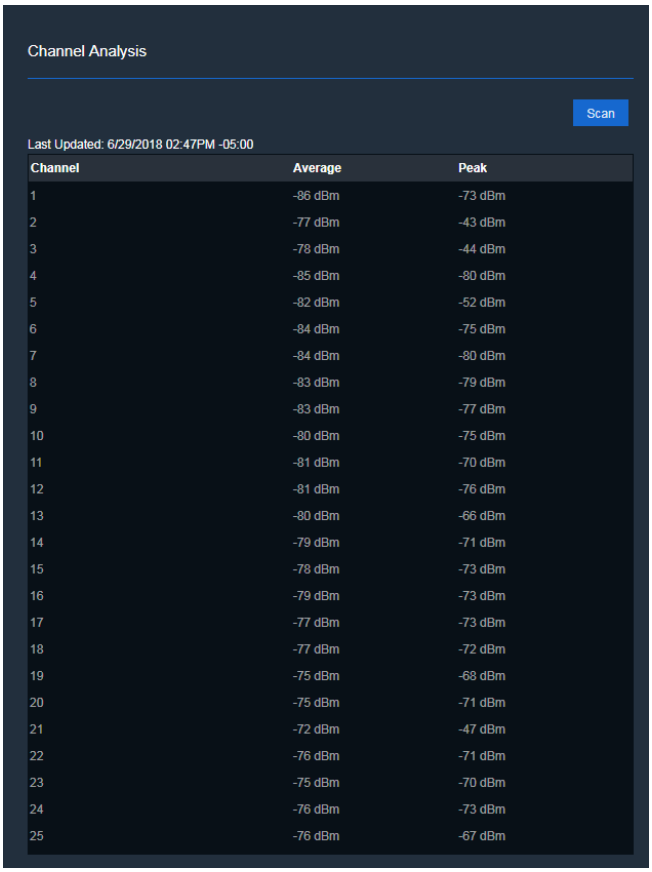


Figure 4.7 Site Analysis Scan (FLR-1000 Example Shown)

The site analysis report shows the average and peak noise power for each supported channel (refer to *Table 4.2* for corresponding frequencies). This information is valuable when selecting the network operating channel for the SEL-FLR installation.

For best results, consider the readings from more than one Channel Analysis scan. Select the channel with the lowest (most negative) Average dBm value. In cases where there are multiple channels with similar low Average readings, select the channel that also has the highest (least negative) Peak dBm value. A higher peak to average power ratio indicates a shorter duty cycle for interfering signals.

Switching SEL-FLR Networks

Each SEL-FLT can be joined with only one SEL-FLR network at a time. In order for an SEL-FLT to join a different SEL-FLR network, it must unjoin from the current SEL-FLR and then establish a communications link with the new SEL-FLR. To unjoin an SEL-FLT from its original SEL-FLR network, remove its Device Address from the whitelist by clicking **Delete**, as shown in *Figure 4.8*.

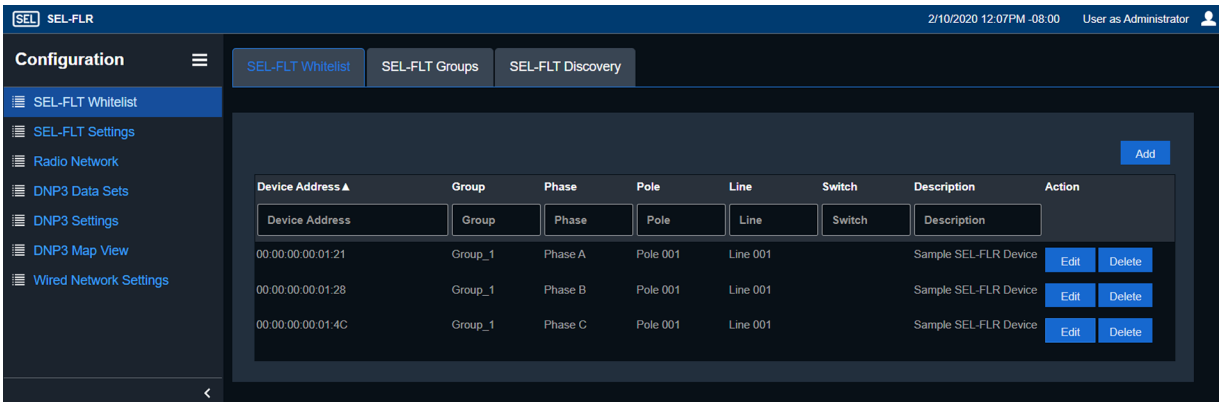


Figure 4.8 Remove SEL-FLT From Whitelist

The SEL-FLR on the original network will stop acknowledging any messages from the removed SEL-FLT. The SEL-FLT will enter the unjoined state 15 minutes later and begin looking for a network. When the SEL-FLT finds the new SEL-FLR network, its Device Address will appear on the Discovery list along with the latest RSSI information for that link. Verify that the SEL-FLT has sufficient link margin to the new SEL-FLR and add that Device Address to the whitelist. Once the SEL-FLT Device Address is present on the whitelist, the SEL-FLT will join that network. If the SEL-FLT cannot join the SEL-FLR network, it will begin its back-off sequence (see *Back-Off* on page 4.4).

Changing RF Channel

When changing the SEL-FLR network RF channel to avoid interference, all joined SEL-FLT devices will lose communication with the SEL-FLR. After changing the RF channel, the SEL-FLT devices on the network will become unjoined from the SEL-FLR after not receiving three consecutive poll messages. Each SEL-FLT will begin searching all channels for an SEL-FLR network. When the SEL-FLT finds the SEL-FLR network on a new channel, a new communications link is established after a few minutes.

Disabling the SEL-FLR Radio

The SEL-FLR radio can be disabled from the **Radio Network** page in the user interface, as shown in *Figure 4.7*. Any joined SEL-FLT devices will sense the stop in communications from the SEL-FLR and begin counting lost message attempts. If the SEL-FLR radio remains off for 15 minutes, the SEL-FLT devices will unjoin the network and begin searching for another network to join following the back-off sequence described in *Back-Off* on page 4.4.

Firmware Upgrade Performance

NOTE: If an SEL-FLR network has more than 96 SEL-FLT devices in the whitelist, a firmware upgrade to R104 or later will remove excess SEL-FLT devices from the whitelist until the list is reduced to 96 SEL-FLT devices. Use a second SEL-FLR to re-establish communications with these excess SEL-FLT devices.

The SEL-FLR is able to upgrade firmware and settings for the SEL-FLT devices via an over-the-air upgrade. See *Firmware Upgrade Instructions* on page 5.13 for details.

While a firmware upgrade is in progress, the SEL-FLR continues to receive fault and load messages. The SEL-FLT devices receiving the firmware upgrade also continue normal operation during the upgrade. Upon finishing a firmware download, the SEL-FLT devices will install the firmware and restart.

SEL-FLR Front-Panel LEDs

The SEL-FLR front panel is equipped with radio status LEDs (shown in *Figure 4.9*) to indicate radio and SEL-FLT network status. *Table 4.3* describes the different statuses shown by the radio status LEDs.

The **LINK QUALITY** LEDs indicate the RSSI value of the last SEL-FLT message received by the SEL-FLR. These LEDs may fluctuate with each message received by the SEL-FLR depending on the link quality with the SEL-FLT.

Figure 4.9 Front-Panel Radio Status LEDs

Table 4.3 Front-Panel Radio Status LED Descriptions

Label	Color	Description
LINK	Green	At least one SEL-FLT is joined with the SEL-FLR.
	Yellow	The radio network is enabled, but no SEL-FLT devices are joined.
	Off	The SEL-FLR radio is disabled.
ACT	Green	Illuminates each time the SEL-FLR receives data from an SEL-FLT.
	Off	No data are being received from SEL-FLT devices.
LINK QUALITY	Green (fourth LED)	Excellent link quality—RSSI is greater than –60 dBm.
	Green (third LED)	Good link quality—RSSI is between –76 dBm and –60 dBm.
	Yellow (second LED)	Fair link quality—RSSI is between –86 dBm and –75 dBm.
	Red (first LED)	Poor link quality—RSSI is less than –86 dBm.
	Off (all LEDs)	The SEL-FLR radio is disabled, no SEL-FLT devices are connected, or there is insufficient data to determine link quality.

Dashboard

SEL-FLR Dashboard

The SEL-FLR Dashboard includes an overview of the wireless network under the SEL-FLT Network Status heading, as shown in *Figure 4.10*. This includes the radio status, a comparison of the number of joined devices versus the number of SEL-FLT devices on the whitelist, and the status of any in-progress firmware upgrades being sent over-the-air to SEL-FLT devices.

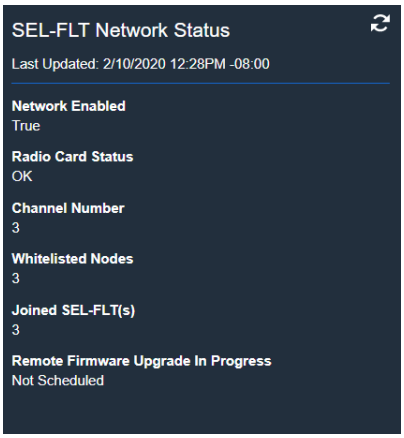


Figure 4.10 Dashboard View of Network Status

SEL-FLT Dashboard

The SEL-FLT Dashboard provides comprehensive diagnostic information about each SEL-FLT joined to the network. The SEL-FLT Dashboard page shows a list of all the devices on the whitelist, including their description, status, and last activity date. Click on an SEL-FLT to show all network statistics for that device, as shown in *Figure 4.11*, including the number of radio transmissions and received signal strength indicator (RSSI) data. See *SEL-FLT Message Types and Data* on page 7.12 for details about device information.

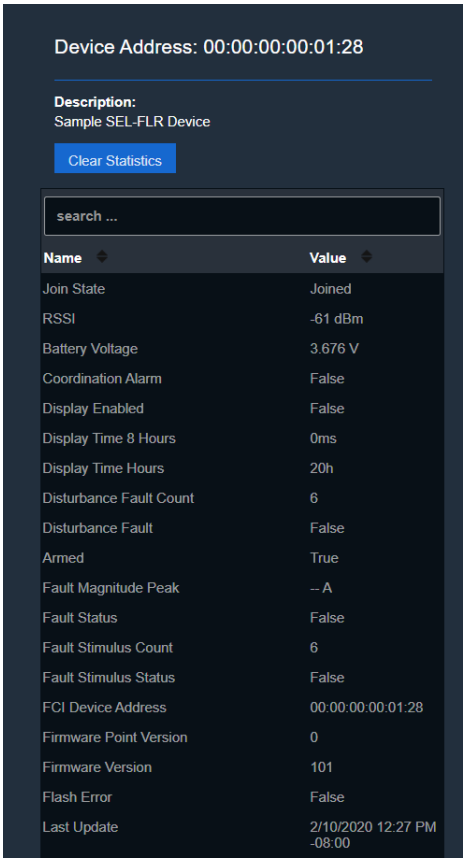


Figure 4.11 SEL-FLT Dashboard Device Statistics

SEL-FLT Sensor Management

The SEL-FLR Fault and Load Receiver provides the interface for management and monitoring of SEL-FLT Fault and Load Transmitters that are joined with the wireless network.

The sensor management operations are performed through a wireless connection between the SEL-FLR and each SEL-FLT, typically after the SEL-FLT has been installed on the power line. See *Getting Started* on page 2.21 for instructions on connecting to the SEL-FLR and configuring its whitelist to allow SEL-FLT devices to join with it.

Each SEL-FLT exists as an independent entity and can be managed individually or in groups from the Sensors tab.

Each SEL-FLR network is set up and managed through the use of a whitelist. To access the whitelist, navigate to the **Configuration > SEL-FLT Whitelist** page on the SEL-FLR web interface.

Discovery list

Navigate to the **SEL-FLT Discovery** tab at the top of the Whitelist page. The list shows all of the unjoined SEL-FLT devices that are able to transmit a join request to the SEL-FLR. Note that the presence of an SEL-FLT on the discovery list is not a guarantee that it will be able to successfully join the SEL-FLR network and maintain a reliable communication link.

Any SEL-FLT that is unjoined will periodically broadcast its status to all SEL-FLR Receivers, indicating that it is available to join with. The Discovery list will show all devices within range that have a status of unjoined as well as the time stamps of their last message. Devices on the Discovery list only share their unjoined status, and will not transmit data to the SEL-FLR. The Discovery list is persistent through web sessions. This list is cleared automatically after an SEL-FLR power cycle or restart, and can also be manually cleared via the **Clear Discovered SEL-FLTs** button.

Whitelist

The whitelist is a table of the SEL-FLT devices, identified by Device Address, that are allowed to join the SEL-FLR network. To prevent unauthorized devices from joining, *only* SEL-FLT devices that are explicitly listed in the whitelist are allowed to join. To add or remove an SEL-FLT from the whitelist, navigate to the **SEL-FLT Whitelist** tab on the SEL-FLR web interface, as shown in *Figure 4.12*.

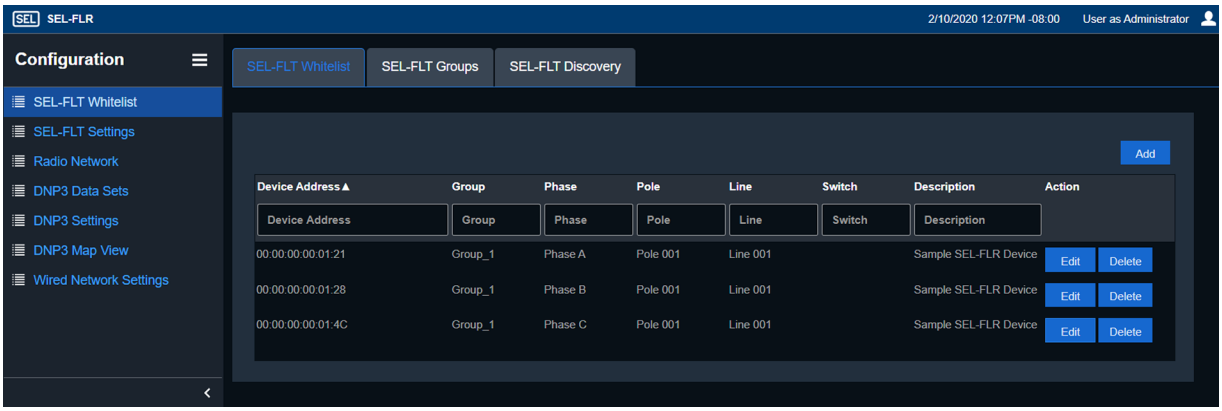


Figure 4.12 SEL-FLT Whitelist Page

Adding SEL-FLT Devices

Only SEL-FLT devices on the whitelist will establish a communications link and transmit sensor data to the SEL-FLR. See *Section 4: SEL-FLR Configuration* for details about how a link is established.

To manually add an SEL-FLT to the whitelist, click **Add**, enter the unique Device Address for the SEL-FLT and any of the attribute fields, and click **Submit**, as shown in *Figure 4.13*.

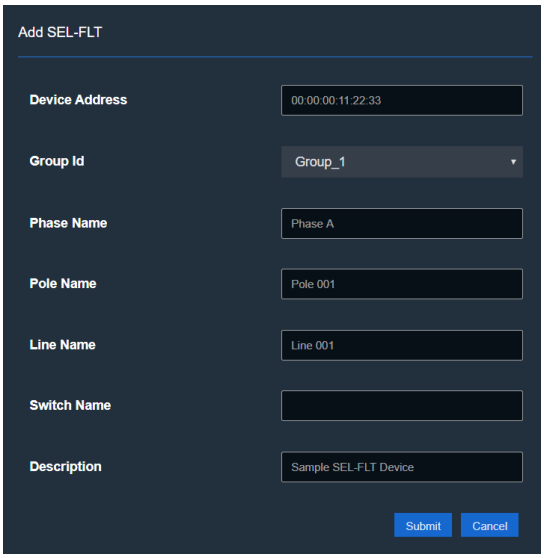


Figure 4.13 Manually Adding an SEL-FLT to a Whitelist

NOTE: The time stamps in the Discovery list are in Coordinated Universal Time (UTC).

The SEL-FLT devices shown in the Discovery list can also be added to the whitelist. Select an SEL-FLT device from the Discovery list and click **Add to Whitelist**, as shown in *Figure 4.14*. Once an SEL-FLT is added to the whitelist, it will be removed from the Discovery list (i.e., an SEL-FLT cannot simultaneously appear in both the Discovery list and the whitelist).

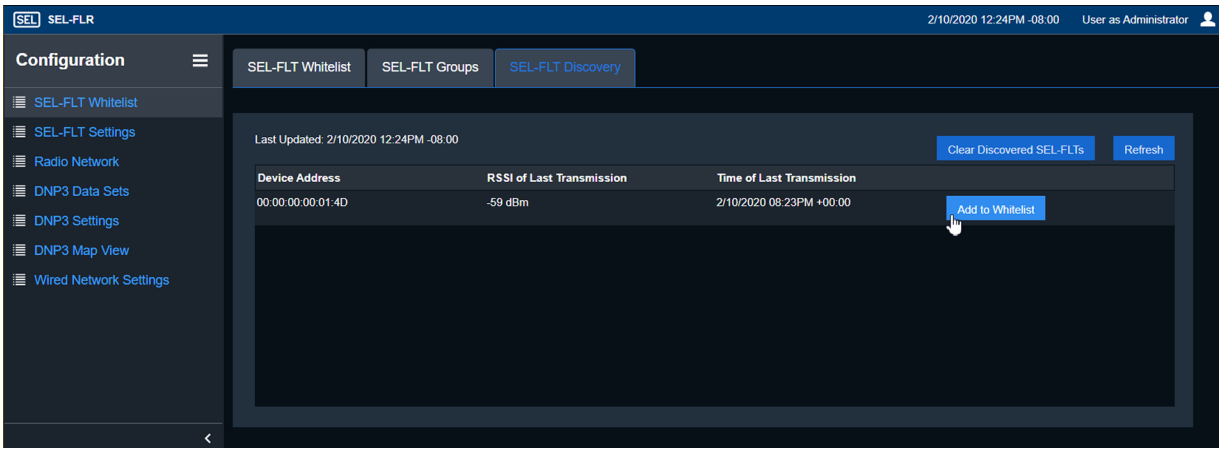


Figure 4.14 Adding an SEL-FLT From the Discovery List to the Whitelist

Device Attributes

Each SEL-FLT on the whitelist has associated attribute fields to provide a description of that device (as shown in *Figure 4.13*). These attributes can be entered when adding devices to the whitelist manually, or from the whitelist at any time by clicking the **Edit** button.

Table 4.4 describes the attribute fields available for each device in the whitelist. The attributes are optional fields that provide convenience for organizing and sorting devices, and they have no effect on the system operation. The same entry may be used for more than one SEL-FLT. For example, if three SEL-FLT devices are installed at the same pole, they may have the same value in the Pole field.

Table 4.4 Whitelist Attribute Fields

Attribute	Values	Description
Required Entries		
ID	1–96	A unique number identifying each SEL-FLT (assigned by the SEL-FLR).
Device Address	Fixed 12-digit number	A unique number identifying each SEL-FLT device (assigned at the factory). This attribute is not user-configurable.
Optional Entries		
Group	1–255 characters	Suggested use: add to an existing Group. A group must be created before an SEL-FLT can be added to it.
Phase	0–32 characters	Suggested use: define the phase on which the SEL-FLT is installed.
Pole	0–32 characters	Suggested use: define the pole number on which the SEL-FLT is installed.
Switch	0–32 characters	Suggested use: define the switch number on which the SEL-FLT is installed.
Line	0–32 characters	Suggested use: define the line on which the SEL-FLT is installed.
Notes	0–253 characters	Suggested use: add any notes about the SEL-FLT (e.g., street name).

Groups

Groups allow for customized sorting and organization of devices in the whitelist. There is no limit to the number of devices in a group. Before you can assign devices to a group, you must create a group. Navigate to the **Configuration > SEL-FLT Whitelist > SEL-FLT Groups** tab and click **Add** to create a group. Enter a unique group name, as shown in *Figure 4.15*. After a group is created, you will be able to select that group name for any SEL-FLT in the whitelist.

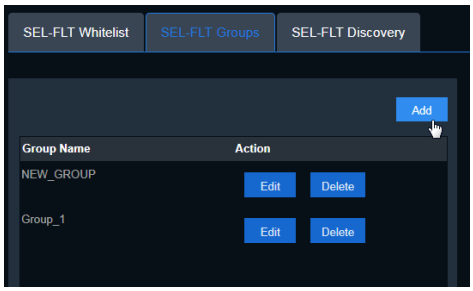


Figure 4.15 Create Group Attribute

Ethernet Network Interfaces

The SEL-FLR Ethernet network interfaces provide connectivity for device management, DNP3 communications, and remote status and event reporting.

The SEL-FLR has two rear-panel network ports (ETH 1 and ETH 2) for normal network connections and one interface on the front panel (ETH F) for local management of the device. The front-panel and rear-panel network interfaces are independent of one another. ETH 1 and ETH 2 share one IP address and can pass network traffic between themselves.

ETH F operates in Layer 3 mode with an assigned IP address and the HTTPS service enabled for management of the device. ETH 1 and ETH 2 are not enabled in the default state.

IP services (HTTPS, DNP3, and Captive Port) are enabled per-interface, and a service may only be available on specific interfaces. For example, Captive Port is only available on the ETH F interface. An IP address must be assigned to an interface before IP services can be enabled and activated on that interface.

This section includes the following:

ETH F Interface Reset

The SEL-FLR includes a pinhole reset button to reenable the ETH F interface and services (HTTPS) on that interface. This may be necessary for situations in which ETH F, ETH 1, and ETH 2 are disabled or restricted from accessing the SEL-FLR because of an inadvertent IP configuration settings change.

NOTE: Do not press the pinhole reset button while turning on the SEL-FLR. This will reset the SEL-FLR to factory-default conditions.

Perform the following steps while the SEL-FLR is in operation to reset the ETH F interface.

Step 1. Locate the pinhole reset button (next to ETH F).

Step 2. Insert a pin or paper clip into the hole and gently press the reset button for at least 5 seconds.

Captive Port

Captive Port is a service that combines a subset of Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) applications to assist with automatic network configuration of devices connected to a port. A network device (typically a computer) with the DHCP client enabled will, when connected to the interface with Captive Port enabled, receive an IP address, a default gateway and a limited DNS resolver. This will resolve all DNS requests to the address the Captive Port configuration designates.

To use the Captive Port feature for managing the SEL-FLR, connect a DHCP client-enabled computer to the SEL-FLR ETH F port. Wait a few minutes for the service to complete its configuration, and then open a web browser. Enter any site name (selinc.com, for example) into the address bar. The browser automatically redirects to the commissioning page (non-commissioned device) or to the login page (commissioned device).

Captive Port on the SEL-FLR is intended to supply an IP address to one device directly connected to the ETH F port. It is not meant to supply IP addresses to a network of devices. If the ETH F port is connected to a network, the Captive Port option should be disabled.

Captive Port assigns IP addresses to the DHCP client according to the IP address configuration of the ETH F interface. A change of IP address on the ETH F interface causes Captive Port reconfiguration and results in it assigning addresses based on the new settings. The client must request a new DHCP lease to continue working. It is typically easiest to disconnect and reconnect the cable from ETH F to accomplish this.

HTTPS

HTTPS allows a client web browser to connect to the device to manage configuration settings. This service is enabled independently for ETH F and for the paired ETH 1 and ETH 2 interface.

To prevent loss of management access to the device, at least one interface with an IP address and HTTPS enabled must be enabled at all times.

DNP3

DNP3 is a standard communications protocol used in SCADA systems to remotely monitor end devices. DNP3 allows the SCADA system to perform data collection and telecontrol.

DNP3 is one of the protocols included in the IEEE 1379-2000, *Recommended Practice for Data Communication between Remote Terminal Units and Intelligent Electronic Devices in a Substation*. See *Appendix B: DNP3 Profile and Data Map* for DNP3 configuration details.

Ping

NOTE: The SEL-FLR Ethernet ports do not allow incoming ping (echo requests) in firmware version R102-V0 and earlier.

To aid in configuring network settings, the SEL-FLR interface can be configured to respond to ping requests. This service is enabled independently for **ETH F** and for the paired **ETH 1** and **ETH 2** interface.

Settings

Access the Ethernet Network Interface settings by navigating to **Configuration > Wired Network Settings** on the SEL-FLR web interface, as shown in *Figure 4.16*.

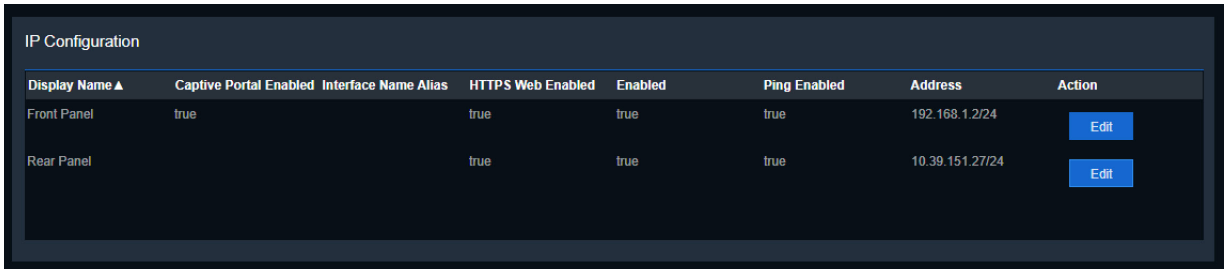


Figure 4.16 Ethernet Network Interface Settings

The Network Interface settings must adhere to the following IP address guidelines:

- All IP addresses defined on the device are IPv4 addresses.
- All IP addresses must be in the range of 1.0.0.0–223.255.255.254.
- Interface IP addresses cannot be the network or broadcast address (first or last address in the address range the mask defines).
- Front-panel interface (**ETH F**) and rear-panel interface IP addresses must be unique. The rear-panel interface (**ETH 1** and **ETH 2**) share the same IP address.
- Interface IP addresses cannot have the same network address (first address in the address range the mask defines).
- Interface IP address cannot be the same as a remote Syslog server or DNP3 client address.
- Only one DNP Session can be anonymous.
- If multiple DNP sessions are enabled and one session is configured for anonymous DNP functionality, the anonymous session must be the highest-numbered session for reliable operation of all sessions.
- **ETH F** requires an IP address even when the port is disabled. This is to support the front-panel management port reset option.

Table 4.5 General Network Settings

Setting Name	Value	Default	Description
Hostname	1–63 characters	SelDeviceHostName	The unique name identifying the device on the network.
Default IPv4 Gateway	Unicast IP address		The IP address of the device used to transfer packets to another network.

Table 4.6 shows the Network Interface settings for the **ETH F** interface, and *Table 4.7* shows the same information for the **ETH 1** and **ETH 2** interface. The settings are presented separately because the default values and available settings differ between the front-panel and rear-panel interfaces.

The Port Settings tab allows you to enable or disable the **ETH F**, **ETH 1**, and **ETH 2** ports on the device.

Table 4.6 ETH F Network Interface Settings

Setting Name	Value	Default	Description
Enabled	Checked, Unchecked	Checked	Enables or disables the interface.
Alias	1–32 characters		Associates a name with the network interface.
IP Address	Unicast IP address	192.168.1.2/24	Establishes the IP address of the interface. The device uses classless inter-domain routing (CIDR) notation to assign the subnet mask.
HTTPS	Checked, Unchecked	Checked	Enables or disables HTTPS on the interface.
Captive Port	Checked, Unchecked	Unchecked	Enables or disables Captive Port on the interface.
Ping	Checked, Unchecked	Unchecked	Enables or disables ping requests on the interface.

Table 4.7 ETH 1 and ETH 2 Network Interface Settings

Setting Name	Value	Default	Description
Enabled	Checked, Unchecked	Unchecked	Enables or disables the interface.
Alias	1–32 characters		Associates a name with the network interface.
IP Address	Unicast IP address		Establishes the IP address of the interface. The device uses classless inter-domain routing (CIDR) notation to assign the subnet mask.
HTTPS	Checked, Unchecked	Unchecked	Enables or disables HTTPS on the interface.
Ping	Checked, Unchecked	Unchecked	Enables or disables ping requests on the interface.

Front Panel

Interface LEDs

Each physical Ethernet port (**ETH F**, **ETH 1**, and **ETH 2**) contains two status LEDs collocated with the port. The green LED indicates connection and activity, and the yellow LED indicates speed and collision. The SEL-FLR also includes front-panel **100Mbps** and **LINK/ACT** LEDs (as shown in *Figure 4.17*) that mimic the status of the rear-panel ports.

Figure 4.17 Front-Panel Ethernet Port LEDs

Table 4.8 describes the port status LED indications.

Table 4.8 Port Status Indicators

Indicator LED	Color	On	Blinking	Off
LINK/ACT	Green	Link present; no activity	Link present; transmit/receive activity	Link absent or interface disabled
100Mbps	Yellow	100 Mbps link	Data collision	10 Mbps link, link absent, or interface disabled

Dashboard

The SEL-FLR Dashboard web interface provides a graphical indication of the status of the Ethernet interfaces and ports on the device. The color of the icon indicates whether the interface or port is enabled or disabled. The symbol next to the icon indicates if the port is enabled, disabled, or enabled but lacking a connection to an Ethernet device.

When the icon is green, as shown in *Figure 4.18*, the port is enabled. The check box symbol next to the icon shows that an Ethernet device is connected. The warning symbol indicates that the port is enabled, but no Ethernet device is connected.

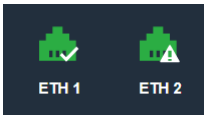


Figure 4.18 Ethernet Dashboard Indicators: Enabled

When the icon is light gray, as shown in *Figure 4.19*, the port or interface is disabled.

Figure 4.19 Ethernet Dashboard Indicators: Disabled

DNP Communication

The SEL-FLR provides a DNP3 Level 2 Outstation interface for direct network connections to the SEL-FLR.

This section includes the following:

Introduction to DNP3

A SCADA manufacturer developed DNP3 from the lower layers of IEC 60870-5. Originally designed for use in telecontrol applications, version 3 of the protocol has also become popular for local substation data collection. DNP3 has been standardized as IEEE 1815.

Rather than wiring individual input and output points from the station remote terminal unit (RTU) to the station IEDs, many stations use DNP3 to convey measurement and control data over a single serial or Ethernet cable to the RTU. The

RTU then forwards data to the offsite master station. By using a data communications protocol rather than hard wiring, designers have reduced installation, commissioning, and maintenance costs while increasing remote control and monitoring flexibility.

The DNP User's Group maintains and publishes DNP3 standards in cooperation with IEEE. See the DNP User's Group website (dnp.org) for more information on DNP3 standards, implementers of DNP3, and tools for working with DNP3.

DNP3 Specifications

DNP3 is a feature-rich protocol with many ways to accomplish tasks. The *Interoperability* section of IEEE 1815 defines four levels of subsets to help improve interoperability. These levels are listed in *Table 4.9*.

Table 4.9 DNP3 Implementation Levels

Level	Description	Equipment Types
1	Simple: limited communications requirements	Meters, simple IEDs
2	Moderately complex: monitoring and metering devices and multifunction devices that contain more data	Protective relays, RTUs
3	Sophisticated: devices with great amounts of data or complex communications requirements	Large RTUs, SCADA masters
4	Enhanced: additional data types and functionality for more complex requirements	Large RTUs, SCADA masters

Each level is a proper superset of the next lower-numbered level. A higher-level device can act as a master to a lower-level device, but can only use the data types and functions implemented in the lower-level device. For example, a typical SCADA master is a Level 3 device and can use Level 2 (or lower) functions to poll a Level 2 (or lower) device by using only the data types and functions that the lower-level device uses. A lower-level device can also poll a higher-level device, but the lower-level device can only access the features and data available to its level.

Data Handling

Objects

DNP3 uses a system of data references called object types, commonly referred to as objects. Each subset level specification requires a minimum implementation of objects and also recommends several optional objects. DNP3 objects are specifications for the type of data the object carries. An object can include a single value or more complex data. Some objects serve as shorthand references for collections of data or even all data within the DNP3 device.

Each instance of the object includes an index that makes it unique. For example, each binary status point (Object 1) has an index. If there are 16 binary status points, these points are Object 1, Index 0 through Object 1, Index 15. Note that index numbers are 0-based.

Each object also includes multiple versions called variations. For example, Object 1 has three variations: 0, 1, and 2. Variation 0 is used to request Object 1 data from a DNP3 device by using its default variation, Variation 1 is used to specify binary input values only, and Variation 2 is used to specify binary input values with status information.

Each DNP3 device has both a list of objects and a map of object indices. The list of objects defines the available objects, variations, and qualifier codes. The map defines the indices for objects that have multiple instances and what data or control points correspond with each index.

A master initiates all DNP3 message exchanges except unsolicited data. DNP3 terminology describes all points from the perspective of the master. Binary points for control that move from the master to the outstation are called binary outputs, while binary status points within the outstation are called binary inputs.

Function Codes

Each DNP3 message includes a function code. Each object has a limited set of function codes that a master may use to manipulate the object. The object listing for the device shows the permitted function codes for each type of object. The most common DNP3 function codes are listed in *Table 4.10*.

Table 4.10 Selected DNP3 Function Codes

Function Code	Function	Description
1	Read	Request date from the outstation
2	Write	Send data to the outstation
3	Select	First part of a select-before-execute operate
4	Execute	Second part of a select-before-execute operate
5	Direct operate	One-step operation with acknowledgment
6	Direct operate, no ack.	One-step operation with no acknowledgment

Qualifier Codes and Ranges

DNP3 masters use qualifier codes and ranges to make requests for specific objects by index. Qualifier codes specify the style of range, and the range specifies the indices of the objects of interest. DNP3 masters use qualifier codes to compose the shortest, most concise message possible when requesting points from a DNP3 remote.

For example, the qualifier code 01 specifies that the request for points will include a start address and a stop address. Each of these two addresses uses 2 bytes. An example request that uses qualifier code 01 might have the four-hexadecimal byte range field, 00h 04h 00h 10h, that specifies points in the range of 4–16.

DNP3 in the SEL-FLR

The SEL-FLR is a DNP3 Level 2 Outstation device that can communicate with one DNP3 client (or master station). The SEL-FLR supports DNP3 LAN/WAN in which you can use any of the Ethernet ports. DNP3 over a direct serial connection is not supported at this time.

The SEL-FLR DNP3 interface supports the following capabilities:

- Event data reporting or unsolicited data
- Time-tagged data
- Time synchronization
- Analog deadband settings

- Multiple sessions
- Anonymous session

Data Access

DNP3 has many features that help it obtain maximum possible message efficiency. DNP3 masters send requests with the least number of bytes by using special objects, variations, and qualifiers that reduce the message size. Other features eliminate the continual exchange of static (unchanging) data values. These features optimize the use of bandwidth and maximize performance over a connection of any speed.

DNP3 event data collection eliminates the need to use bandwidth to transmit values that have not changed. Event data are time-stamped records that show when observed measurements changed. For binary points, the outstation device logs changes from logical 1 to logical 0 and from logical 0 to logical 1. For analog points, the remote device logs changes that exceed a deadband. DNP3 outstation devices collect event data in a buffer that either the master can request or the device can send to the master without a request message. Data sent from the outstation to the master without a polling request are called unsolicited data.

DNP3 data fit into one of four event classes: 0, 1, 2, or 3. Class 0 is reserved for reading the present value (static data). Classes 1, 2, and 3 are event data classes. The meaning of Classes 1 to 3 is arbitrary and defined by the application at hand. With remotes that contain great amounts of data or in large systems, the three event classes provide a framework for prioritizing different types of data. For example, you can poll once a minute for Class 1 data, once an hour for Class 2 data, and once a day for Class 3 data.

Class 0 polling is also known as static polling, or simple polling of the present value of data points within the outstation. By combining event data polls, unsolicited messaging, and static polling, you can operate your system in one of the four access methods shown in *Table 4.11*.

The access methods listed in *Table 4.11* are in order of increasing communications efficiency. With various trade-offs, each method is less demanding of communications bandwidth than the previous one. For example, unsolicited report-by-exception consumes less communications bandwidth because of the elimination of polling messages from the master required by polled report-by-exception. You must also consider the overall system size and the volume of data communication expected to properly evaluate which access method provides optimum performance for your application.

Set the data access method by configuring the SEL-FLR DNP3 Master settings, as shown in *Table 4.11*.

Table 4.11 DNP3 Access Methods and Corresponding SEL-FLR Settings (Sheet 1 of 2)

Access Method	Master Polling	SEL-FLR Settings
Polled static	Class 0	Binary Event Data Class = OFF Counter Event Data Class = OFF Analog Event Data Class = OFF Unsolicited Reporting Enabled = Disable
Polled report-by-exception	Class 0 occasionally; Class 1, 2, 3 frequently	Binary Event Data Class = Desired class Counter Event Data Class = Desired class Analog Event Data Class = Desired class Unsolicited Reporting Enabled = Disable

Table 4.11 DNP3 Access Methods and Corresponding SEL-FLR Settings (Sheet 2 of 2)

Access Method	Master Polling	SEL-FLR Settings
Unsolicited report-by-exception	Class 0 occasionally; optional Class 1, 2, 3 less frequently; mainly relies on unsolicited messages	Binary Event Data Class = Desired class Counter Event Data Class = Desired class Analog Event Data Class = Desired class Unsolicited Reporting Enabled = Enable Unsolicited Reporting at Power up Enabled = Enable or Disable
Quiescent	Class 0, 1, 2, 3 never; relies completely on unsolicited messages	Binary Event Data Class = Desired class Counter Event Data Class = Desired class Analog Event Data Class = Desired class Unsolicited Reporting Enabled = Enable Unsolicited Reporting at Power up Enabled = Enable

In both the unsolicited report-by-exception and quiescent polling methods shown in *Table 4.11*, you must make a selection for the Unsolicited Reporting at Power up Enabled setting. If your master can send the DNP3 message to enable unsolicited reporting from the SEL-FLR, set Unsolicited Reporting at Power up Enabled to **Disable**.

While automatic unsolicited data transmission when the device turns on is convenient, problems can result if your master is not prepared to start receiving data at that time. If the master does not acknowledge the unsolicited data with an acknowledgment Application Confirm, the SEL-FLR will resend the data until it is acknowledged. Additionally, masters with insufficient processing power may encounter dropped data when many devices simultaneously send data and expect acknowledgment messages.

DNP3 LAN/WAN Considerations

The main process for carrying DNP3 over an Ethernet network (LAN/WAN) involves encapsulating the DNP3 data link layer data frames within the transport layer frames of the IP suite. This allows the IP stack to deliver the DNP3 data link layer frames to the destination in place of the original DNP3 physical layer.

The DNP User's Group Technical Committee has recommended the following guidelines for carrying DNP3 over a network:

- DNP3 shall use the IP suite to transport messages over a LAN/WAN
- Ethernet is the recommended physical link, though others may be used
- TCP must be used for WANs
- TCP is strongly recommended for LANs
- UDP may be used for highly reliable, single-segment LANs
- UDP is necessary if broadcast messages are required
- The DNP3 protocol stack shall be retained in full
- Link layer confirmations shall be disabled

The Technical Committee has registered a standard port number, 20000, for DNP3 with the Internet Assigned Numbers Authority (IANA). This port is used for either TCP or UDP.

The Committee recommends the selection of TCP or UDP protocol as per the guidelines in *Table 4.12*.

Table 4.12 TCP/UDP Selection Guidelines

Use in the case of...	TCP	UDP
Most situations	X	
Non-broadcast or multicast	X	
Mesh Topology WAN	X	
Broadcast		X
Multicast		X
High-reliability, single-segment LAN		X
Pay-per-byte, non-mesh WAN (e.g., Cellular Digital Packet Data [CDPD])		X
Low-priority data (e.g., data monitor or configuration information)		X

While the Transport Protocol is set to UDP, the Data Link Heartbeat Timeout automatically configures to 0. When the Transport Protocol is switched from UDP to TCP, the Data Link Heartbeat Timeout automatically configures to the default setting (120 seconds).

Event Data

DNP3 event data objects contain change-of-state and time-stamp information that the SEL-FLR collects and stores in a buffer. You can configure the SEL-FLR to either report the data without a polling request from the master (i.e., unsolicited data) or to hold the data until the master requests them with an event poll message.

With the settings Binary Event Data Class, Counter Event Data Class, and Analog Event Data Class, you can set the event class for each data type. You can use the classes as a simple priority system for collecting event data. The SEL-FLR responds to independent class poll requests but treats all classes identically in unsolicited messages.

For event data collection, you can either use default deadband and scaling settings or configure these settings according to data type. For example, with a scaling setting of 0, the value of 12.632 would be sent as 13. With a scaling setting of 1, the value transmitted is 126. With a scaling setting of 3, the value transmitted is 12632. Regardless of the scaling value, the maximum value transmitted cannot exceed 32767 if you are polling the default 16-bit variations for Objects 30 and 32 (but you can send some decimal values by using this technique). You must also configure the master to perform the appropriate division on the incoming value to display it properly.

Application of event reporting deadbands occurs after scaling in the settings. For example, if you set Current Scaling Decimal Places to 2 and Analog Reporting Deadband for Currents to 10, a measured current of 10.14 A would be scaled to the value 1014. The measurement would have to increase to more than 1024 or decrease to less than 1004 (a deadband of 0.2 A [scaled to 20]) for the SEL-FLR to report a new event value.

The SEL-FLR uses the Number of Events to Transmit On and Age of Oldest Event to Transmit On settings to decide when to send unsolicited data to the master. The SEL-FLR sends an unsolicited report when the total number of events accumulated in the event buffer reaches the value of Number of Events to Transmit On.

The SEL-FLR also sends an unsolicited report if the age of the oldest event in the buffer exceeds Age of Oldest Event to Transmit On.

Time Synchronization

DNP3 can provide time synchronization for the SEL-FLR. This is sufficient for applications that require timing to be accurate on the order of seconds.

NOTE: Only one DNP3 client can be configured at a time.

Enable time synchronization with the DNP3 Time and Time Set Request Interval settings and use Object 50, Variation 3 for DNP3 LAN/WAN to set the time via a DNP3 master.

Configure the SEL-FLR time synchronization in one of the following ways:

- The SEL-FLR requests a time synchronization format from the client at a specific rate:

  DNP Time Enabled = **ENABLE**
  Time Set Request Interval = **1–32767**

- The SEL-FLR accepts and applies time from the client (prohibits requesting time synchronization):

  DNP Time Enabled = **ENABLE**
  Time Set Request Interval = **0**

- The SEL-FLR ignores time synchronization from the client (prohibits requesting time synchronization):

  DNP Time Enabled = **DISABLE**

DNP3 Settings

DNP3 Master (Client) Session Settings

Access the DNP3 Protocol settings by navigating to **Configuration > DNP3 Settings** on the SEL-FLR web interface.

Table 4.13 shows the settings fields of the DNP3 Master settings for each DNP session.

Table 4.13 Ethernet Port DNP3 Protocol Settings (Sheet 1 of 2)

Name	Range	Default
Communication		
Transport Protocol	TCP, UDP	TCP
Client IP Address	—	192.168.1.100
UDP Response Port	1025–3000, 3002–65534	20000
TCP/UDP Port Number	1025–65534	20000
Time		
DNP Time Enabled	Enable, Disable	Disable
Time Set Request Interval	0–32767 minutes	1
DNP		
Client DNP Address	0–65519	0
Server DNP Address	0–65519	1
Binary Event Data Class	OFF, 1–3	1
Counter Event Data Class	OFF, 1–3	1
Analog Event Data Class	OFF, 1–3	1
Current Scaling Decimal Places	0–3	0

NOTE: The UDP Response Port cannot be set to 3001.

Table 4.13 Ethernet Port DNP3 Protocol Settings (Sheet 2 of 2)

Name	Range	Default
Voltage Scaling Decimal Places	0–3	0
Miscellaneous Scaling Decimal Places	0–3	0
Default Variations of Analog Inputs	1–6	5
Analog Reporting of Deadband for Currents	0–32767	100
Analog Reporting of Deadband for Voltages	0–32767	100
Control Options Enabled	Enable, Disable	Disable
Number of Events to Transmit On	1–200	10
Event Message Confirm Timeout	1–50 seconds	2
Age of Oldest Event to Transmit On	0–99999 seconds	2
Select Operate Timeout	0–60 seconds	1
Data Link Heartbeat Timeout	0–7200 seconds	120
Unsolicited Reporting Enabled	Enable, Disable	Disable
Unsolicited Reporting at Power Up Enabled	Enable, Disable	Disable
Unsolicited Message Max Retries	2–10	8
Unsolicited Message Offline Timeout	1–5000 seconds	60

Anonymous DNP Master (Client) Connection

NOTE: For DNP Sessions 1–3, the IP address of 0.0.0.0 is for anonymous DNP. Anonymous DNP is only supported for TCP protocol. If anonymous DNP is used, it must be the highest-numbered DNP session.

NOTE: If a DNP3 master disconnects from any anonymous session and a different DNP3 master then connects, the SEL-FLR will not re-send previously acknowledged DNP3 events.

The SEL-FLR supports as many as three DNP sessions. You can set one of the three sessions to accept anonymous connections from a DNP master station.

The SEL-FLR accepts an anonymous DNP3 connection request from any DNP3 master whose address is not configured for another session.

When an anonymously connected DNP3 master disconnects from the anonymous session, the session is available for a new connection. Any DNP3 master that requests a connection (whose address is not explicitly set elsewhere) will connect to the anonymous session. DNP3 events and class polls are associated with the sessions, not with any particular DNP3 master.

DNP3 Data Sets

The SEL-FLR DNP3 data sets are mapped into a block with configurable starting and ending addresses for each data type (e.g., Binary Inputs, Analog Inputs, Counters, etc.). Access the DNP3 Block Settings by navigating to the **Configuration > DNP3 Data Sets** page and selecting the **DNP3 Blocks** tab on the SEL-FLR web interface, as shown in *Figure 4.20*. Click **Edit** and set the starting and ending address for each of the data types. Click **Submit** to apply changes.

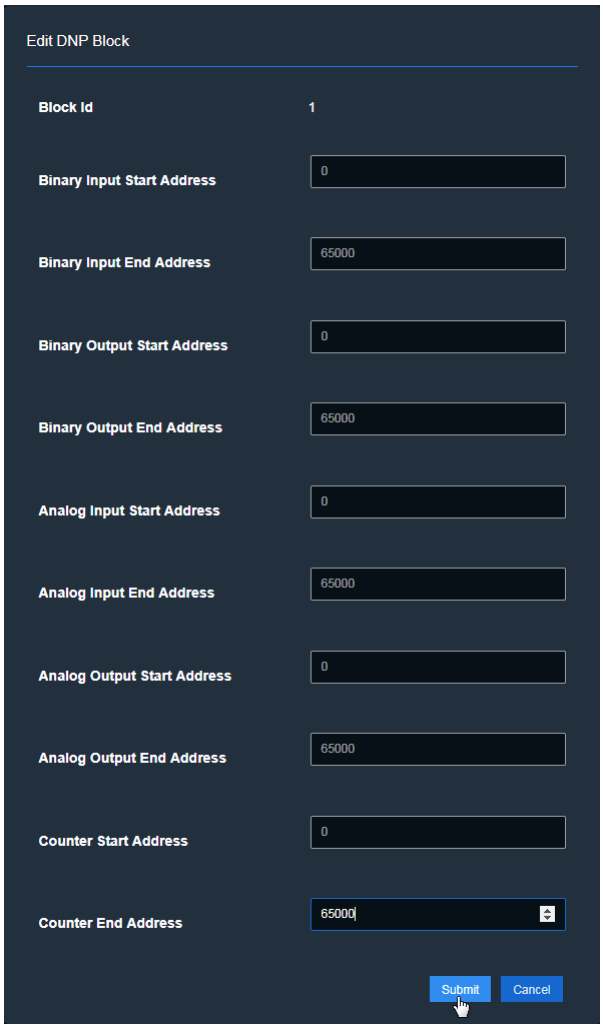


Figure 4.20 DNP3 Address Setup

The default data maps, shown in *Table B.2*, define the data points for each of the three supported components (the SEL-FLR, the SEL-FLR radio, and the SEL-FLT). From the **DNP3 Data Sets** tab, select a device listed in the **Unmapped Devices** table and click **Submit** to map to the block, as shown in *Figure 4.21*. When you add a device to a block, the SEL-FLR automatically checks if the DNP3 data points of the component fit within the unused addresses at the end of any previously mapped components. The SEL-FLR rejects the insertion of a component if the number of data points of the component exceeds the number of unused addresses.

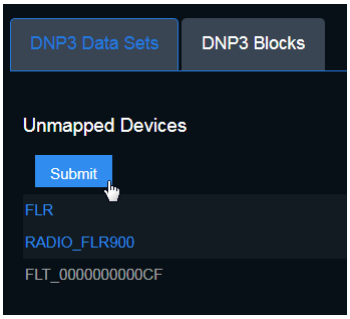


Figure 4.21 Adding a Device to the DNP3 Map

Component Removal and Block Remap

NOTE: If an SEL-FLR network has more than 96 SEL-FLT devices in the whitelist, a firmware upgrade to R104 or later will remove DNP3 data sets of the excess SEL-FLT devices.

NOTE: Remapping may affect the addressing of one or several components. To avoid mismatched data for a system in operation, remapping should be coordinated with the administrator of the DNP3 client (a SCADA system engineer, for example).

The **DNP3 Data Sets** settings page allows you to remove a component by selecting the component and clicking **Remove**. Once a component is removed, the SEL-FLR reserves the address values of the removed component with default values. This means that other components in that block will not be reassigned new addresses when a device is removed. Following removal of a component, any new components that are added will not be inserted at the vacated addresses but will instead be added to the end of the existing map.

Clicking **Remap** reallocates the reserved addresses from the removed components and compacts the data points of remaining components. The SEL-FLR will not remove or readjust the addresses of any removed components until you remap the block.

SEL-FLT Parameters and Settings

This section contains details of all user-configurable settings in the SEL-FLT. The SEL-FLR web interface is used to maintain and remotely modify SEL-FLT settings for all devices on the SEL-FLR network. The default values will suit most applications, allowing the SEL-FLT to operate as a fault and load monitor without requiring any settings changes. Changing the SEL-FLT settings allows for optimizing the device performance for specific applications.

This section includes the following:

SEL-FLT Settings

On the SEL-FLR web interface, navigate to the **Configuration** menu to access the **SEL-FLT Settings** page. All SEL-FLT settings for devices on the network are viewed and managed from this page. The pane on the left shows a list of all nodes in the whitelist. Select one or more devices to view the settings of the selected transmitters in the pane on the right. When multiple devices are selected that have different settings values, a mixed indication will show next to that setting, as shown in *Figure 4.22*.

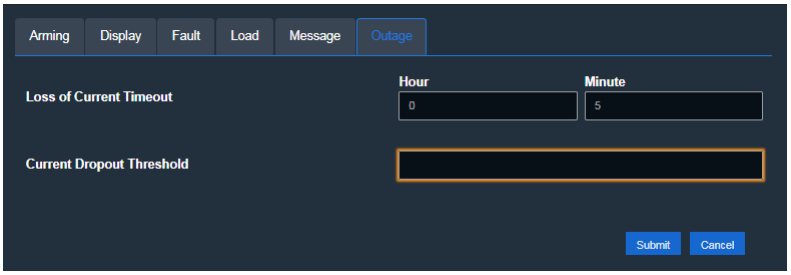


Figure 4.22 Example of Mixed Settings

NOTE: Over-the-air firmware upgrades take priority over a settings update. Therefore, a settings update will not be pushed until after the firmware upgrade window is complete.

To change settings, select a device or devices from the list of SEL-FLT devices and click **Edit Selected**. Changing a mixed setting will apply to all selected devices. Click **Submit** to apply any changes. After you submit a settings change, the affected devices will automatically receive an over-the-air update with the new settings. Settings pushes typically take 15 minutes, but may take longer depending on other network traffic.

You can back up all SEL-FLT device settings (as well as the SEL-FLR settings) by using the **Import/Export** feature. See *File Management* on page 5.11 for details.

Arming

System Arming Period (T_{ARM})

The System Arming Period (T_{ARM}) parameter defines the duration for which load current must exceed the I_{ARM} threshold before the SEL-FLT arms.

Setting	Default	Range	Increment
T_{ARM}	300 seconds (5 minutes)	15–324000 seconds (90 hours)	15 seconds

Current Arming Threshold (I_{ARM})

The Current Arming Threshold (I_{ARM}) parameter defines the minimum current level that the SEL-FLT must detect before arming.

Setting	Default	Range	Increment
I_{ARM}	5 A	3–600 A	1 A

Enable Arming Hold-Off

The Enable Arming Hold-Off parameter determines whether the SEL-FLT waits for the duration of the Arming Hold-Off Period (T_{HO}) before detecting the arming conditions.

Setting	Default	Range	Increment
Enable Arming Hold-Off	Disabled	Enabled, Disabled	N/A

Arming Hold-Off Period (T_{HO})

The Arming Hold-Off Period (T_{HO}) parameter defines the amount of time following a permanent event that must pass before the SEL-FLT starts detecting the arming conditions. The T_{HO} parameter is only used when the Enable Arming Hold-Off parameter is set to TRUE.

Setting	Default	Range	Increment
T_{HO}	1 hour	1–240 hours (10 days)	1 hour

Display

Permanent Fault Display Time-Out (T_{PFD})

The Permanent Fault Display Time-Out (T_{PFD}) parameter defines the duration for which the local LED display indicates a permanent fault event before the SEL-FLT turns off the display. The SEL-FLT clears the permanent fault display prior to reaching the Permanent Fault Display Time-Out if the arming requirements (e.g., current restoration) are met.

Setting	Default	Range	Increment
T_{PFD}	8 hours	1–48 hours	1 hour

Display Time-Out (T_{DIS})

The Display Time-Out (T_{DIS}) parameter defines the duration for which the local LED display indicates an event (other than permanent fault events) before the SEL-FLT turns off the display. You can configure which events are indicated by the local LED display.

Setting	Default	Range	Increment
T_{DIS}	8 hours	1–48 hours	1 hour

Enable Momentary Fault Display

The Enable Momentary Fault Display parameter determines whether the SEL-FLT enables the local LED display upon detecting a momentary fault event.

Setting	Default	Range	Increment
Enable Momentary Fault Display	Disabled	Enabled, Disabled	N/A

Enable Permanent Loss-of-Current Display

The Enable Permanent Loss-of-Current Display parameter determines whether the SEL-FLT enables the local LED display upon detecting a permanent loss-of-current event.

Setting	Default	Range	Increment
Enable Permanent Loss-of-Current Display	Disabled	Enabled, Disabled	N/A

Enable Disturbance Display

The Enable Disturbance Display parameter determines whether the SEL-FLT enables the local LED display upon detecting a disturbance event.

Setting	Default	Range	Increment
Enable Disturbance Display	Disabled	Enabled, Disabled	N/A

Fault

Enable AutoRANGE Threshold

The Enable AutoRANGE Threshold parameter determines the status of the AutoRANGE trip thresholds used by the SEL AutoRANGER trip logic. At least one AutoRANGE threshold must always be enabled. If only one AutoRANGE Threshold is enabled, the device will operate with a single fixed trip threshold.

Setting	Default	Range	Increment
Enable AutoRANGE Threshold	Threshold 1: Enabled Threshold 2: Enabled Threshold 3: Enabled Threshold 4: Enabled Threshold 5: Enabled Threshold 5: Enabled Threshold 6: Enabled Threshold 7: Enabled Threshold 8: Enabled Threshold 9: Enabled Threshold 10: Enabled	Enabled, Disabled	N/A

AutoRANGE Trip Threshold

The AutoRANGE trip thresholds determine the fault detection level for all of the enabled thresholds. The number of enabled thresholds is determined by the Enable AutoRANGE Threshold settings. Each threshold setting must be set to a higher value than the previous threshold. The SEL AutoRANGER trip logic uses measured load current to determine which AutoRANGE trip thresholds are active. See *AutoRANGER Trip Logic* on page 8.8 for details.

Setting	Default	Range	Increment
AutoRANGE Trip Thresholds	Threshold 1: 25 A Threshold 2: 50 A Threshold 3: 100 A Threshold 4: 200 A Threshold 5: 400 A Threshold 6: 600 A Threshold 7: 800 A Threshold 8: 1000 A Threshold 9: 1200 A Threshold 10: 1600 A	25–1600 A	1 A

AutoRANGE Delay Trip

The AutoRANGE Delay Trip parameter determines the trip response time for each of the enabled AutoRANGE trip thresholds. Each of the AutoRANGE Delay Trip settings must be set to less than or equal to the value of the previous threshold.

Setting	Default	Range	Increment
AutoRANGE Delay Trip	Default Value 1: 3 half-cycles Default Value 2: 3 half-cycles Default Value 3: 3 half-cycles Default Value 4: 3 half-cycles Default Value 5: 3 half-cycles Default Value 6: 3 half-cycles Default Value 7: 3 half-cycles Default Value 8: 3 half-cycles Default Value 9: 3 half-cycles Default Value 10: 3 half-cycles	1–50 half-cycles	1 half-cycle

Fault Time-Out (T_{FLT})

The Fault Time-Out (T_{FLT}) parameter defines the duration after a fault is detected for which the SEL-FLT waits before determining if the fault type is permanent or momentary.

Setting	Default	Range	Increment
T_{FLT}	300 seconds (5 minutes)	15–3600 seconds (1 hour)	15 seconds

Load

Load Peak Window (T_{PEK})

The Load Peak Window (T_{PEK}) parameter defines the duration of the rolling average window used to calculate the peak load measurement for a long update interval.

Setting	Default	Range	Increment
T_{PEK}	15 minutes	1–60 minutes	1 minute

Messages

Long Update Interval (T_{LUI})

The Long Update Interval (T_{LUI}) parameter defines the duration between periodic Long Update Interval messages.

Setting	Default	Range	Increment
T_{LUI}	24 hours	1–240 hours (10 days)	1 hour

Short Update Interval (T_{SUI})

The Short Update Interval (T_{SUI}) parameter defines the duration between periodic Short Update Interval messages.

Setting	Default	Range	Increment
T_{SUI}	60 minutes	5–60 minutes	1 minute

Enable Restoration Messages

The Enable Restoration Messages parameter determines whether the SEL-FLT transmits a Restoration message after detecting a restoration event.

Setting	Default	Range	Increment
Enable Restoration Messages	Enabled	Enabled, Disabled	N/A

Enable Long Update Interval Messages

The Enable Long Update Interval Messages parameter determines whether the SEL-FLT transmits a Long Update Interval message at each long update interval.

Setting	Default	Range	Increment
Enable Long Update Interval Messages	Enabled	Enabled, Disabled	N/A

Enable Short Update Interval Messages

The Short Update Interval Messages parameter determines whether the SEL-FLT transmits a Short Update Interval message at each short update interval.

Setting	Default	Range	Increment
Enable Short Update Interval Messages	Enabled	Enabled, Disabled	N/A

Enable Fault Stimulus Messages

The Enable Fault Stimulus Messages parameter determines whether the SEL-FLT transmits a Fault Stimulus message when a fault stimulus event is detected.

Setting	Default	Range	Increment
Enable Fault Stimulus Messages	Disabled	Enabled, Disabled	N/A

Enable Permanent Fault Messages

The Enable Permanent Fault Messages parameter determines whether the SEL-FLT transmits a Permanent Fault message when a permanent fault event is detected.

Setting	Default	Range	Increment
Enable Permanent Fault Messages	Enabled	Enabled, Disabled	N/A

Enable Momentary Fault Messages

The Enable Momentary Fault Messages parameter determines whether the SEL-FLT transmits a Momentary Fault message when a momentary fault event is detected.

Setting	Default	Range	Increment
Enable Momentary Fault Messages	Disabled	Enabled, Disabled	N/A

Enable Disturbance Messages

The Enable Disturbance Messages parameter determines whether the SEL-FLT transmits a Disturbance message when a disturbance event is detected.

Setting	Default	Range	Increment
Enable Disturbance Messages	Disabled	Enabled, Disabled	N/A

Enable Permanent Loss-of-Current Messages

The Enable Permanent Loss-of-Current Messages parameter determines whether the SEL-FLT transmits a Permanent Loss-of-Current message when a permanent loss-of-current event is detected.

Setting	Default	Range	Increment
Enable Permanent Loss-of-Current Messages	Disabled	Enabled, Disabled	N/A

Enable Momentary Loss-of-Current Messages

The Enable Momentary Loss-of-Current Messages parameter determines whether the SEL-FLT transmits a Momentary Loss-of-Current message when a momentary loss-of-current event is detected.

Setting	Default	Range	Increment
Enable Momentary Loss-of-Current Messages	Disabled	Enabled, Disabled	N/A

Enable Coordination Alarm Messages

The Enable Coordination Alarm Messages parameter determines whether the SEL-FLT transmits a Coordination Alarm message when a miscoordination event is detected.

Setting	Default	Range	Increment
Enable Coordination Alarm Messages	Enabled	Enabled, Disabled	N/A

Outage

Loss-of-Current Time-Out (T_{LOC})

The Loss-of-Current Time-Out (T_{LOC}) parameter defines the duration after a loss of current is detected for which the SEL-FLT waits before determining if the outage type is permanent or momentary.

Setting	Default	Range	Increment
T_{LOC}	5 minutes	1–60 minutes	1 minute

Current Dropout Threshold (I_{DO})

NOTE: The SEL-FLT separately has a fast drop (I_{MIN}) of 3 A with a response time of 75 ms. The I_{MIN} threshold and response time are not configurable.

The Current Dropout Threshold (I_{DO}) parameter defines the current level that the SEL-FLT must measure below before detecting an outage and becoming unarmed. The I_{DO} has a 10-second response time before the SEL-FLT unarms.

Setting	Default	Range	Increment
I_{DO}	3 A	3–600 A	1 A

The I_{DO} threshold is always configured lower than the Current Arming Threshold (I_{ARM}).

This page intentionally left blank

SECTION 5

System

Overview

This section provides information on the SEL-FLR settings interface, including the following:

Date and Time

The SEL-FLR supports both manual date and time adjustment as well as automatic date and time synchronization through the use of DNP3 time objects.

The same date and time information is used for the SEL-FLR network, Syslog reports, and several functions available in the web interface.

This section includes the following:

Date/Time Settings

Access the local time settings by navigating to **System > Date / Time** on the SEL-FLR web interface, as shown in *Figure 5.1*.

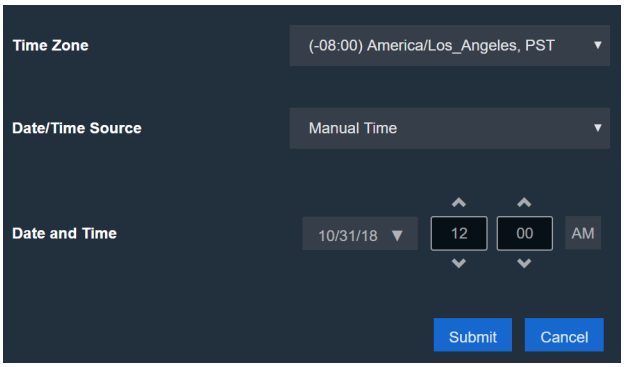


Figure 5.1 Date/Time Settings

Time Source

The SEL-FLR date and time can be either set manually through the web interface or synchronized automatically through the use of DNP3 time objects. Setting the Time Source to DNP3 overrides any manual date and time adjustments. A DNP3 client is required to receive automatic synchronization when using a DNP3 time source. There can be only one DNP time enabled for all sessions. You can choose only one session to receive automatic synchronization from a DNP3 time source.

Set the **Date/Time Source** to either **Manual** or **DNP3** from the drop-down menu and click **Submit** to apply the changes.

Manual Date/Time

When the manual time source is selected, adjust the date and time by using the **Manual Date** and **Manual Time** settings. Select the **Time Zone** offset from UTC from the drop-down menu. Daylight-saving time options are built into the Local Time Zone Offset from UTC settings. Click **Submit** to apply the changes. The manual date and time settings are described in *Table 5.1*.

Table 5.1 Manual Date and Time Settings

Setting Name	Value	Default	Description
Manual Date	MM/DD/YYYY 01/01/2000–12/31/2035	N/A	Manually sets the date. The date will proceed forward from the date you enter.
Manual Time	HH:MM 01:00–12:59 AM/PM	N/A	Manually sets the time. Time will proceed forward from this entered time.

DNP3 Date/Time

The DNP3 time source option configures the SEL-FLR to synchronize date and time through the use of DNP3 time messages. Choose the desired DNP session that will use DNP time. Select a **Time Zone** to offset the DNP3 time source to the local time zone. When the DNP3 time source is already in local time and an offset has already been applied, set the **Time Zone** to UTC (+00.00). See *Time Synchronization* on page 4.25 for more information.

Web Server Settings, Usage Policy, and Contact Information

The SEL-FLR allows for customizing the usage policy message displayed on the login screen and setting the system contact information.

This section includes the following:

Web Server Settings

Use Web Settings to modify settings related to the web management interface of the device. *Table 5.2* lists web settings. Access the web server settings by navigating to **System > Web Server Settings** on the SEL-FLR web interface, as shown in *Figure 5.2*.

Table 5.2 Web Settings

Setting Name	Value	Default	Description
Maximum Sessions	1–20	5	Maximum number of concurrent web user sessions
Session Timeout	1–60 minutes	5	Time a user session is inactive before the device terminates the session

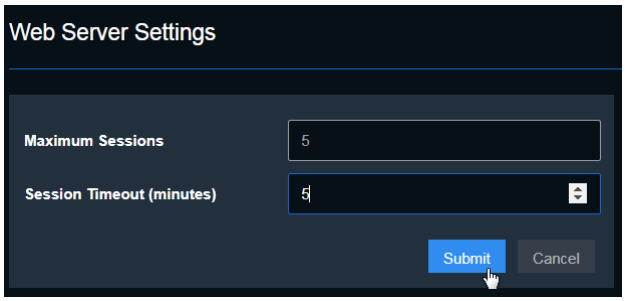


Figure 5.2 Web Server Settings

Usage Policy

The device presents a usage policy to all users accessing the login or commissioning pages. This is a system message that can be changed by the organization. It is designed to notify users regarding what constitutes appropriate use of this device, what actions are necessary to ensure the device is not used inappropriately, and what actions will be taken if abuse is discovered. The device comes with the following default usage policy:

```
This system is for the use of authorized users only. Individuals
using this system without authority, or in excess of their
authority, are subject to having all their activities on this
system monitored and recorded by system personnel. Anyone using
this system expressly consents to such monitoring and is advised
that if such monitoring reveals possible evidence of criminal
activity, system personnel may provide the evidence of such
activity to law enforcement officials.
```

Access the usage policy settings by navigating to **System > Usage Policy** on the SEL-FLR web interface, as shown in *Figure 5.3*. The usage policy is configurable to as many as 4095 characters, and it supports all characters in the UTF-8 character set. Leave the usage policy blank to restore the default usage policy.

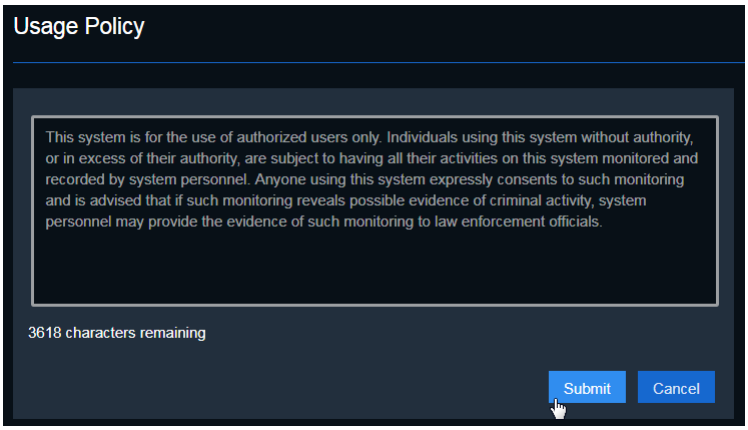


Figure 5.3 Usage Policy Settings

Contact Information

The system contact information settings provide fields for entering a system contact and system location. Access the contact information settings by navigating to **System > Contact Information** on the SEL-FLR web interface, as shown in *Figure 5.4*. *Table 5.3* lists and describes the contact information settings.

Table 5.3 System Contact Information Settings

Setting Name	Value	Default	Description
Contact	0–128 characters	Schweitzer Engineering Laboratories, Inc. (509) 332-1890	Contact information for the device
Location	0–128 characters	Pullman, WA	Location of the device

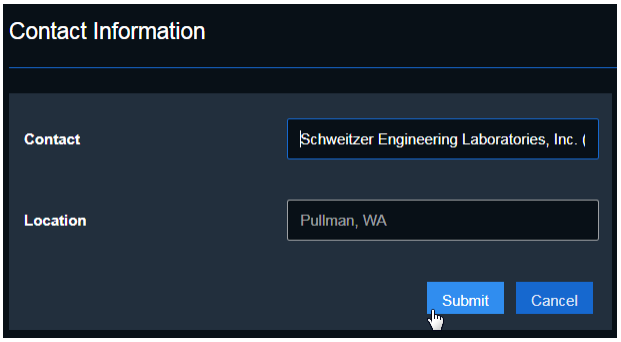


Figure 5.4 Contact Information Settings

Dashboard

System contact and location information appears in the Device Information portion of the SEL-FLR Dashboard page, as shown in *Figure 5.5*.

Figure 5.5 Dashboard Device Information

User Accounts

User accounts allow for engineering access to SEL products. SEL has historically used global accounts, such as Access Level 1 and Access Level 2 (accessible via the **ACC** and **2AC** commands, respectively), to control access.

With global accounts, every user has the same login credentials (username and password), which weakens the security of the system. To strengthen authentication, authorization, and accountability, the SEL-FLR provides a user-based account structure.

The SEL-FLR stores user accounts in nonvolatile memory. This allows the device to maintain account status through power cycles and other unexpected events.

This section includes the following:

Logging in With SEL User-Based Accounts

Upon connection to the SEL-FLR, you are presented with the device usage policy and a login prompt. To log in, enter a valid username and the corresponding password or passphrase. Usernames are case-insensitive and unique to each individual with authority to access the device. Passwords and passphrases are case-sensitive, as shown in *Passphrases* on page 5.8.

If the SEL-FLR determines a username or password to be invalid, it rejects the access attempt and alerts the user that the login credentials were incorrect.

After five failed login attempts within a 5-minute period, the SEL-FLR will block access attempts with that username for 5 minutes. Each failed login attempt generates a Syslog event. Additionally, a Syslog event and minor alarm are generated when an account is locked out after too many failed login attempts. These security features are designed to prevent and slow down password guessing attacks.

Login failure can occur for three reasons: the username was invalid, the password or passphrase was incorrect, or the account of the user is disabled. Check the spelling of the username and password if an access attempt fails. If you are certain that you entered the username and password correctly, contact your system administrator to verify that your account has not been disabled.

Benefits of User-Based Accounts

User-based accounts allow for a stronger security posture than global accounts. User-based accounts have the ability to disable or remove an individual account without affecting access for anyone else.

When password changes are necessary (either because of a compromised system, routine maintenance, or regulatory requirements), users will not need to remember several new and different global passwords. They will only need to remember their own personal password changes. This increases security by reducing both the need to write passwords down and the chance that an unauthorized individual might obtain an active password.

Three key parts of strong access control are authentication, authorization, and accountability. Authentication is the process of verifying user identity. User-based accounts allow for the reliable authentication of individual users of a system. This creates more trust that those who access the system really are whom they claim to be.

Authorization is the process of granting privileges to users of a system. User-based accounts allow you to assign specific privileges to each user of a system.

Accountability is the idea that individual users can be held responsible for their actions on a system. User-based accounts provide the ability to clearly authenticate each user of the system based on their credentials. All actions are tracked to a specific user account, and users can only perform actions allowed by their account privileges. Accountability is very important to event tracking and forensic investigations.

Roles

Device permissions are organized into roles, and access is granted through role-based access controls. The SEL-FLR has four roles: Administrator, Engineer, User Manager, and Monitor. User account privileges are based on the role in which the user is a member. The following list provides a brief overview of each role:

- Administrator: Users have full access to the device.
- Engineer: Users have access to most device settings and information, but cannot access user account management.
- User Manager: Users have access to user account management. Access to other settings is restricted.
- Monitor: Users have read-only access to device settings.

Table 5.4 lists which pages each role has access to.

Table 5.4 User-Based Accounts Role Access

Menu	Page	Administrator	Engineer	Monitor	User Management
Dashboard	SEL-FLR Dashboard	Read	Read	Read	Read
	SEL-FLT Dashboard	Read	Read	Read	Read
Configuration	SEL-FLT Whitelist	Read/Write	Read/Write	Read	None
	SEL-FLT Settings	Read/Write	Read/Write	None	None
	Radio Network	Read/Write	Read/Write	Read	None
	DNP3 Data Sets	Read/Write	Read/Write	Read	None
	DNP3 Settings	Read/Write	Read/Write	Read	None
	DNP3 Map View	Read/Write	Read/Write	Read	None
	Wired Network Settings	Read/Write	Read/Write	Read	Read
System	Date/Time	Read/Write	Read/Write	None	None
	Contact Information	Read/Write	Read	Read	Read
	Usage Policy	Read/Write	Read	Read	None
	Firmware Update	Read/Write	None	None	None
	Change Password	Read/Write	Read/Write	Read/Write	Read/Write
	User Accounts	Read/Write	None	None	Read/Write
	Web Server Settings	Read/Write	Read	Read	None
	Import/Export Settings	Read/Write	None	None	None
	X.509	Read/Write	Read	None	Read
	Syslog	Read/Write	Read	Read	None
	Device Reset	Read/Write	None	None	None
Diagnostics	Local Syslog Events	Read/Write	Read	Read	None
	Alarms	Read/Write	Read	Read	None

Administration of User-Based Accounts

The SEL-FLR is shipped from the factory with no user accounts installed. To access the product, you must create an initial account through the **Device Commissioning** page, as shown in *Figure 5.6*. This account will be an Administrator account, which has the authorization to add, remove, enable, and disable system users. Only the individual who creates this account should have knowledge of this account password.

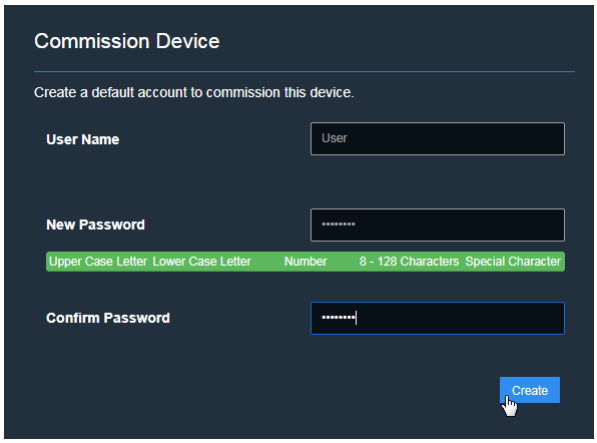


Figure 5.6 Device Commissioning Page

It is possible to create other accounts that can manage users. Only those users with a need to manage user accounts should be a member of the User Manager or Administrator group.

Passphrases

Passphrases provide users the ability to create strong and easy-to-remember passwords that protect access to a system. A strong passphrase includes many different characters from many different character sets. Longer passphrases provide greater security than shorter passphrases. SEL-FLR user-based accounts require complex passphrases that must include the following:

- 8–128 characters
- An uppercase character
- A lowercase character
- A number
- A special character

When you enter a new password, a password policy indicator will appear under the password field to show when the requirements are met, as shown in *Figure 5.7*.

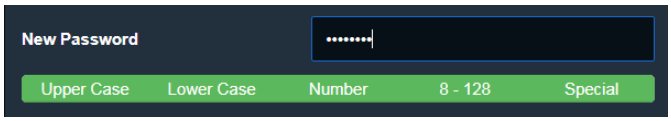


Figure 5.7 Password Policy Indicator

Sample passphrases include the following:

Strong: W3b$ter!

Stronger: A phras3 is 3v3n Str0ng3r!

Users with access to user account management (i.e., Administrator and User Manager roles) can set or change passphrases for any user. Users without such access can only change their own passphrases. For the protection of your account, the SEL-FLR never displays, transmits, or stores a passphrase in plaintext.

Managing User Accounts

This section discusses the settings used to configure and manage local user accounts on the SEL-FLR. If the current (logged in) user has access to user account management (i.e., Administrator or User Management access), access the user accounts settings by navigating to **System > User Accounts** on the SEL-FLR web interface, as shown in *Figure 5.8*.

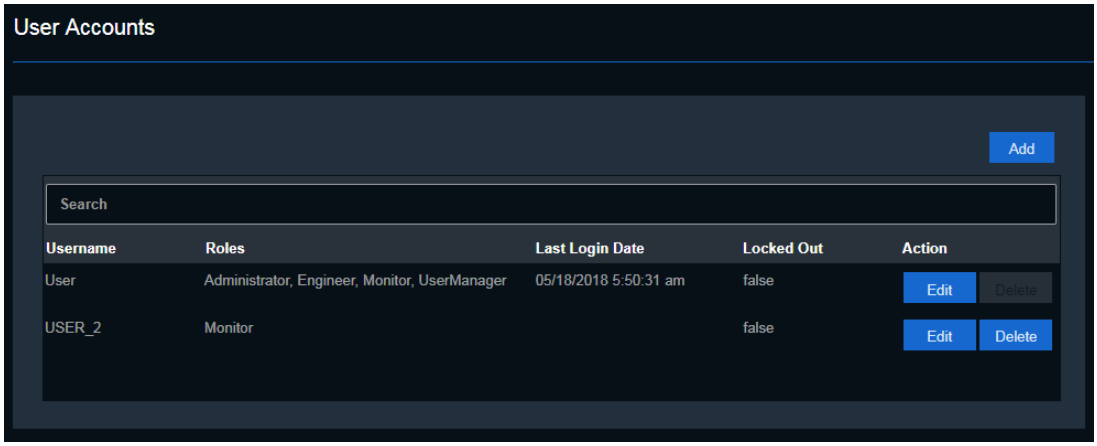


Figure 5.8 User Accounts Management

Add New User

Pressing the **Add** button presents the dialog box for creating a new user, as shown in *Figure 5.8*. Complete all the fields and click **Submit** to create a new user. The Add New User fields are described in *Table 5.5*.

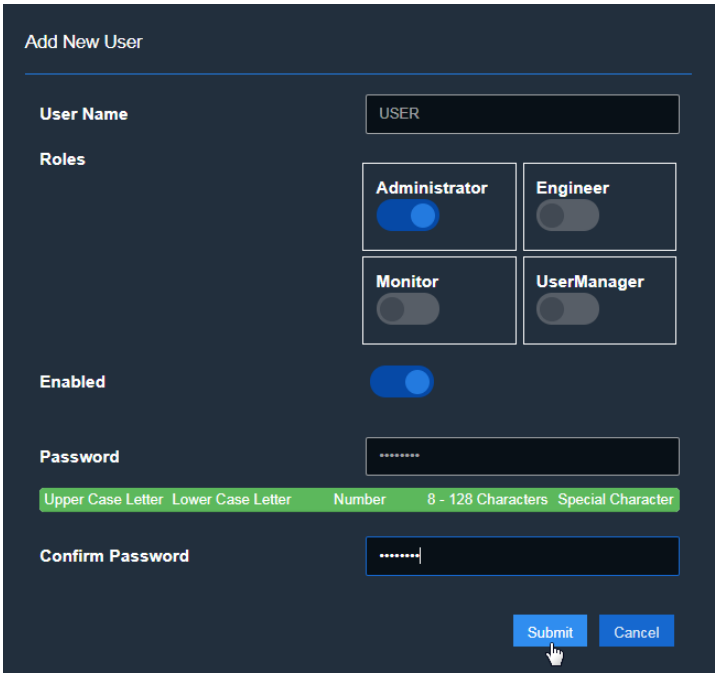


Figure 5.9 Add New User

Table 5.5 Add New User Fields

Setting Name	Value	Default	Description
Username	Printable ASCII characters (as many as 63 characters)		Name that user will use to access device. Name is not case sensitive and will be displayed as lowercase.
Role	Administrator, Engineer, User Manager, Monitor	Administrator	Permission that will be granted to user (see *Roles* on page 5.6).
Password/ Confirm Password	Printable ASCII characters (8–128 characters)		Password for user account. Must be entered in both **Password** and **Confirm Password** fields.
Enabled	Enabled/Disabled	Enabled	Enables or disables the user account.

Edit User

Pressing the **Edit** button associated with a user account presents a dialog box for editing an existing user. This dialog is similar to that for adding a new user, except that the Username field is already defined and cannot be changed.

Delete User

Pressing the **Delete** button associated with a user account presents a dialog box to confirm deletion of that user account.

The SEL-FLR requires that at least one Administrator-level account be available and enabled at all times. If there is only one Administrator-level account on the device, you will not be able to delete or disable that account. While you can *disable* the account used for logging in to the device (if you are currently logged in with this account, you will be immediately logged out after submitting the setting), you cannot *delete* that account.

Change Password

To change the password of the current user, click the user icon and then click **Change Password**, as shown in *Figure 5.10*. This allows the user to change the password on the user account that is currently accessing the SEL-FLR. The new password must meet the password policy as described in *Passphrases* on page 5.8. Click **Submit** to apply the new password settings.

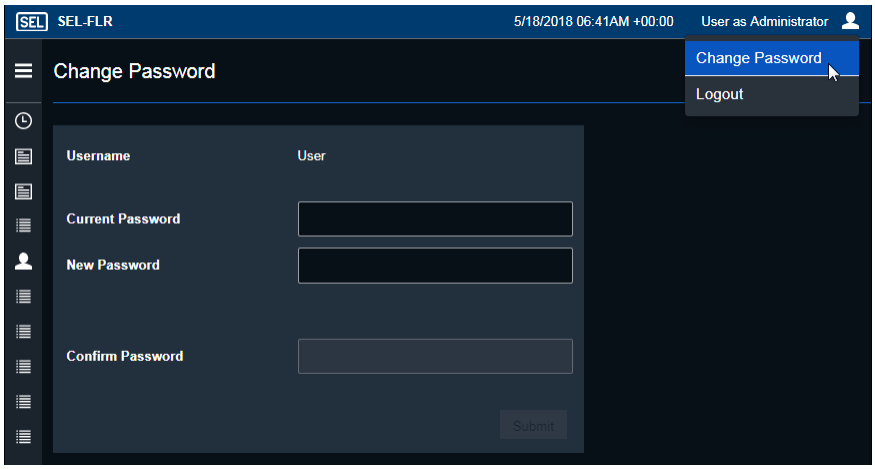


Figure 5.10 Change Password Tab

Dashboard Indications

The current user and role are always displayed in the upper right of the SEL-FLR web interface. You can change the password or log out by clicking the user icon, as shown in *Figure 5.11*.

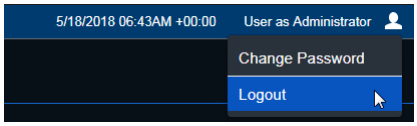


Figure 5.11 Username on Dashboard

File Management

The SEL-FLR manages the backing up of all system settings, including SEL-FLT device settings, and performing firmware upgrades. Exporting system settings is useful for providing device configuration backups for disaster recovery, as well as for creating a template configuration that you can use in commissioning large numbers of devices. For example, if all devices share the same configuration, with the exception of a few device-specific settings such as hostname and IP address, you only need to create the configuration once and then export it as a template. Then, once you import the configuration file into a new device, you only need to make minor changes before the device is fully configured. For a valid configuration, do not import settings files to an SEL-FLR that has a different model number. See *Table 1.1* for a list of SEL-FLR model numbers.

Export Settings

The settings export functionality is useful for creating a copy of the device configuration as a device backup. You can use this copy for disaster recovery purposes in the event of lost device configuration. This is a single backup file that includes all of the SEL-FLR settings and all SEL-FLT settings for devices on the whitelist.

Settings can be exported in either an encrypted or unencrypted format.

Access the Import/Export settings by navigating to **System > Import/Export Settings** on the SEL-FLR web interface, as shown in *Figure 5.12*.

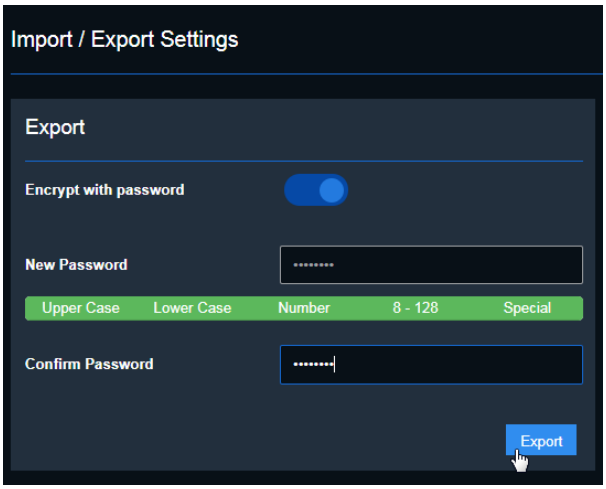


Figure 5.12 Export Tab

Step 1. To export settings in an encrypted format, enable the **Encrypt with password** setting and enter an encryption password for use in encrypting the settings file. The password must meet the password policy requirements provided in *Passphrases* on page 5.8. You must use the password to perform an import of the encrypted settings file, so be sure you store it in a secure location.

To export settings in an unencrypted format, disable the **Encrypt with password** setting.

NOTE: Store unencrypted settings files in a secure location if they contain sensitive information.

Step 2. Click **Export**.

Step 3. The settings export initializes and automatically downloads to your local computer. The device displays the following message when the export is complete.

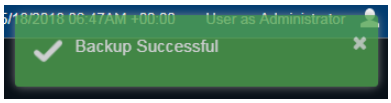


Figure 5.13 Export Complete

Import Settings

NOTE: Importing settings replaces the present settings and restarts the device.

NOTE: A settings import file created on an SEL-FLR that used firmware earlier than R104 and has more than 96 SEL-FLT devices in the whitelist will be accepted, but the excess SEL-FLT devices will be dropped from the whitelist. A second SEL-FLR is required to establish communications with the remaining SEL-FLT devices.

NOTE: Importing a settings file that was created on an SEL-FLR that used firmware earlier than R104 will result in the syslog being cleared.

Importing settings allows you to restore the SEL-FLR with a backup file. Importing settings will replace existing settings on the device and cannot be undone. Importing settings will cause the device to restart.

Access the Import/Export settings by navigating to **System > Import/Export Settings** on the SEL-FLR web interface, as shown in *Figure 5.12*.

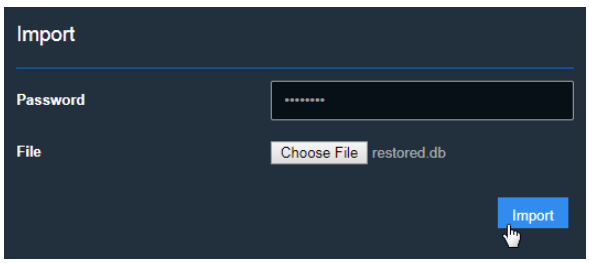


Figure 5.14 Import Settings Tab

Step 1. Click **Choose File** and navigate to the location of the settings file you want to import.

Step 2. If the file was encrypted during the export process, enter the encryption password into the **Password** field. If the file was not encrypted during the export process, leave the **Password** field blank.

Step 3. Click the **Import** button.

Once the device successfully imports settings, the SEL-FLR will automatically restart to apply the restored settings.

Firmware Upgrade Instructions

NOTE: Read and understand all the firmware upgrade instructions before attempting any firmware upgrade.

SEL occasionally offers firmware upgrades to enhance or improve the performance of devices.

Both the SEL-FLT and SEL-FLR support firmware upgrades, and both store the firmware image in nonvolatile memory.

The SEL-FLR firmware upgrade is managed by the web interface. The SEL-FLT firmware upgrade is also managed by the web interface, but the firmware file is transmitted to the SEL-FLT devices over a wireless connection.

These instructions provide a step-by-step procedure for upgrading the device firmware by uploading a firmware file from a personal computer via the web interface, and the common procedure to use the File Management interface to select and transfer firmware to both the SEL-FLT and SEL-FLR systems.

To perform an upgrade, you need the appropriate firmware upgrade file and access to an administrative account on the device.

Firmware Files

SEL-FLR firmware upgrade files have a tar.gz extension. An example firmware file name is *install_FLR_R100.tar.gz*.

SEL-FLT firmware upgrade files have a tar.gz extension. An example firmware file name is *install_FLT_R100.tar.gz*.

The firmware packages are cryptographically signed so that the device can recognize official SEL firmware. The device will not process any files it uploads for which it cannot verify SEL as the file creator.

SEL-FLR Firmware Upgrade

NOTE: Upgrading SEL-FLR firmware from any version earlier than R104 to version R104 or later will result in the syslog being cleared.

NOTE: Upgrading SEL-FLR firmware from any version earlier than R104 to version R104 or later, reduces the maximum number of SEL-FLT in the network to 96 devices. Network size will be limited to 96 SEL-FLT devices and excess SEL-FLT devices will be dropped from the network. A second SEL-FLR is required to establish communications with the remaining SEL-FLT devices.

Do not attempt to start a firmware upgrade for the SEL-FLR while an SEL-FLT firmware upgrade is currently in progress. Doing so will result in a loss of data. Before starting an SEL-FLR firmware upgrade, either wait for the SEL-FLT firmware upgrade to finish or terminate the SEL-FLT firmware upgrade.

Access the SEL-FLR Firmware Upgrade page by navigating to **System > Firmware Upgrade** on the SEL-FLR web interface, as shown in *Figure 5.15*.

Perform the following steps to upgrade the SEL-FLR firmware:

Step 1. Select the **SEL-FLR** tab at the top of the page to display the current firmware version on the SEL-FLR, as shown in *Figure 5.15*.

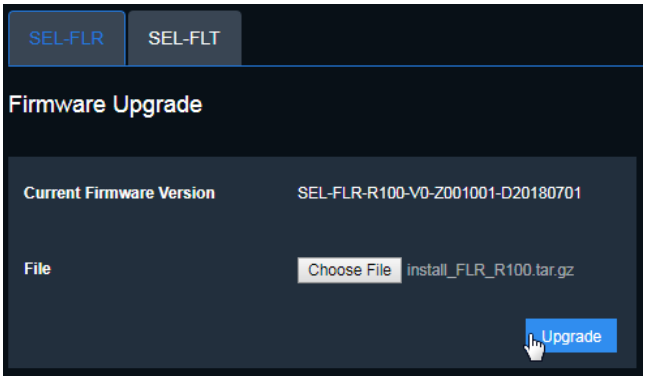


Figure 5.15 SEL-FLR Firmware Upgrade

Step 2. Click **Choose File** and navigate to the location where the upgrade file is stored. Select the file and click **Open**.

Step 3. Click **Upgrade** at the bottom of the dialog box to upload and install the new firmware. Completion of an SEL-FLR firmware upgrade takes approximately 30–40 minutes.

After the firmware upgrade, the SEL-FLR can take an additional 30 minutes to restart and reload its applications. Do not restart the SEL-FLR during this time.

SEL-FLT Firmware Upgrade

Firmware upgrades for SEL-FLT devices are managed by the SEL-FLR. After an SEL-FLT firmware upgrade is started by the SEL-FLR, the firmware upgrade file is distributed to all joined SEL-FLT devices via an over-the-air download. The firmware upgrade file is downloaded by SEL-FLT devices over a long period of time in small pieces, so normal network operation and functionality is maintained during the download. This means fault and load data will still be received while a firmware upgrade file is being downloaded.

Firmware upgrades for SEL-FLT devices typically take approximately 4–7 days but they may take longer depending on network conditions. The progress for each device being upgraded is shown on both the Firmware Upgrade page and the SEL-FLT Dashboard page. The progress of the overall download is shown on the Firmware Upgrade page.

The SEL-FLT will validate all firmware upgrade files before installing them. The SEL-FLT will only download firmware upgrade files that are a newer release than that currently running on the SEL-FLT.

After an SEL-FLT downloads and installs a new firmware file, it will perform a reset and briefly unjoin the SEL-FLR network. The SEL-FLT will automatically rejoin the SEL-FLR network after resetting. When the SEL-FLT rejoins the network, it will indicate that it is running the new firmware version. The SEL-FLT will initially be unarmed after a reset and must rearm before being able to detect fault events.

Access the SEL-FLT firmware upgrade page by navigating to **System > Firmware Upgrade** on the SEL-FLR web interface, as shown in *Figure 5.16*.

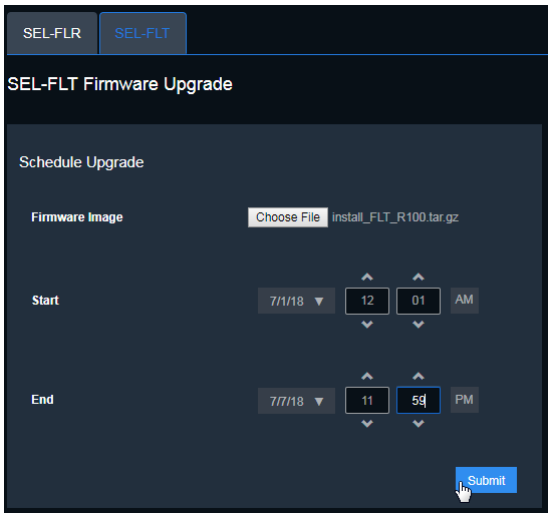


Figure 5.16 SEL-FLT Firmware Upgrade

Perform the following steps to upgrade the SEL-FLT firmware:

Step 1. Click the SEL-FLT tab at the top of the page, as shown in *Figure 5.16*.

Step 2. Click **Choose File** and navigate to the location where the upgrade file is stored. Select the file and click **Open**.

Step 3. Select a starting date and time for when the SEL-FLR will start distributing the firmware upgrade file to joined SEL-FLT devices.

Step 4. Select an ending date and time for when the SEL-FLR will stop distributing the firmware upgrade file.

Step 5. Click **Submit** to begin uploading and installing the new firmware.

The firmware upgrade status for each SEL-FLT on the network will be displayed, as shown in *Figure 5.17*.

An SEL-FLT firmware upgrade can be terminated by clicking **Cancel**.

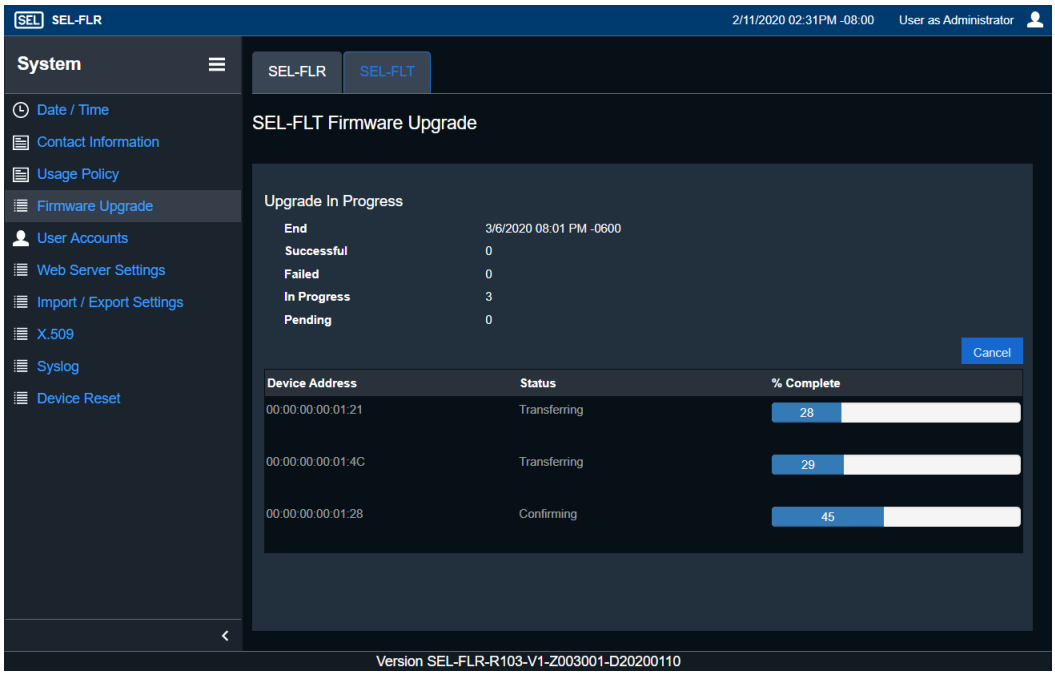


Figure 5.17 SEL-FLT Firmware Upgrade Status

Dashboard

SEL-FLR Dashboard

The SEL-FLR Dashboard displays the current firmware version in the Device Information section, as shown in *Figure 5.18*.

Figure 5.18 SEL-FLR Device Information

SEL-FLT Dashboard

The SEL-FLT Dashboard displays the current firmware version and firmware point version on each SEL-FLT device independently. Click an SEL-FLT device to show all of the device details. In the search bar, type **firmware** to find the SEL-FLT firmware version, as shown in *Figure 5.19*.

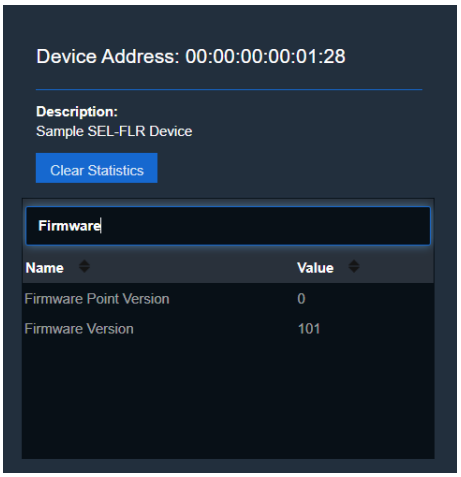


Figure 5.19 SEL-FLT Device Information

X.509 Certification Management

HTTPS (SSL/TLS) connections must be authenticated to confirm that the user is communicating with the correct server. In the SEL-FLR, this authentication is provided by an X.509 certificate. The device automatically generates the initial, self-signed certificate. Because the certificate is self-signed, a connecting client web browser may issue a security alert. This alert requires a security exception before authentication can continue.

The initial, self-signed certificate can be replaced with an organization-generated X.509 server certificate signed by your organization or a trusted Certificate Authority (CA). Replacing the default certificate with a CA-signed certificate that the client web browser trusts will remove the security alert caused by the initial self-signed certificate.

Certificates have defined start and end dates. After the certificate end date, the browser provides a warning that the certificate has expired.

Certificates have a public key and a private key. Both are necessary before a client device trusts the certificate and allows communication with the server. All devices connecting to the SEL-FLR web management interface receive the public key. Only the owner of each device has the private key specific to that device. If a private key is compromised or distributed to unauthorized personnel, replace all certificates corresponding to that key.

For an overview and examples on the function of X.509 certificates, see *Appendix E: X.509*.

X.509 Certificates

Access the X.509 settings by navigating to **System > X.509** on the SEL-FLR web interface, as shown in *Figure 5.20*.

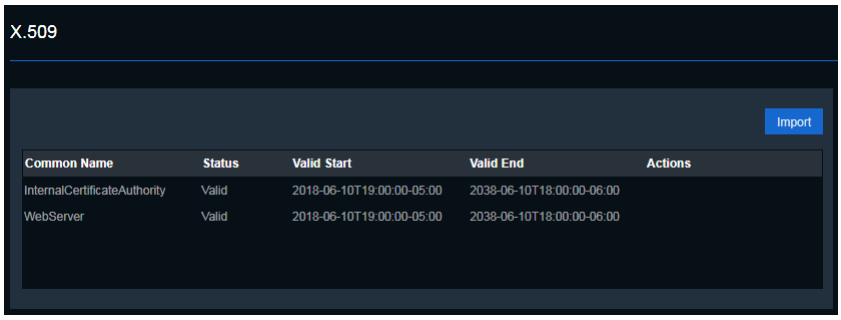


Figure 5.20 X.509 Certificates

Import Certificate

The **Import** button allows you to add a new web server certificate to the SEL-FLR, as shown in *Figure 5.21*. Click **Choose File** and browse to the certificate you want to add, change the **Purpose** to WebServer, enter the certificate password (if necessary), and then click **Submit**. Once a new certificate is uploaded, the SEL-FLR will automatically revoke the previous certificate. Only one Web Server certificate is active at a time.

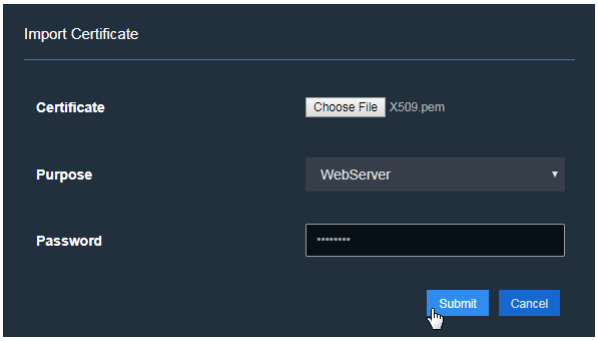


Figure 5.21 X.509 Import Certificate

Device Reset

The SEL-FLR can be restarted or reset through the use of the web interface or the pinhole reset.

This section includes the following:

Web Interface Device Reset

The SEL-FLR has two options for resetting or restarting the device. You can choose to perform a basic device restart or a factory-default reset. Access the Device Reset settings by navigating to **System > Device Reset** on the SEL-FLR web interface, as shown in *Figure 5.22*.

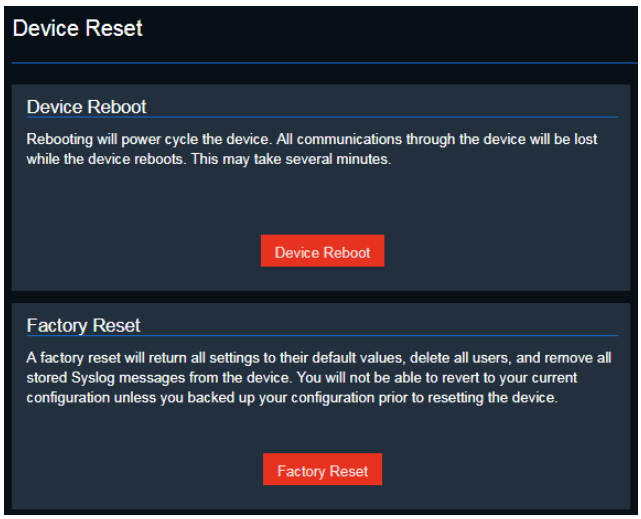


Figure 5.22 Device Reset Web Interface

Device Reboot

Restarting will power cycle the SEL-FLR. All communication through the device will be lost while the device restarts, and it may take several minutes to reestablish communications links with previously joined SEL-FLT devices. A restart operation does not affect SEL-FLR or SEL-FLT settings, communications options, or wireless network configuration.

Factory Reset

NOTE: The factory reset function is intended for local use. Using the function via remote access is not recommended because Ethernet configurations will be reset to default values.

Performing a factory reset decommissions the SEL-FLR.

A factory reset returns all settings to their default values, deletes all users, removes all devices from the whitelist, and removes all stored Syslog messages from the device. You will not be able to revert to your previous configuration unless you back up your configuration prior to resetting the device.

Because all settings are reset (including communications settings and local user account credentials), the web session terminates after a factory reset.

Pinhole Reset

NOTE: If the front port has been configured for a subnet other than 192.168.1.*x* and the rear port has been configured to a 192.168.1.*x* address, a pinhole reset to reset the front port will not reset the front port to its default address.

The SEL-FLR front panel includes a pinhole reset (shown in *Figure 5.23*) with two functions: the first is to reset the front-panel Port F (**ETH F**) functionality, and the second is to reset the SEL-FLR settings to factory defaults.

Figure 5.23 Front-Panel Pinhole Reset

ETH F Interface Reset

The pinhole can be used to reset the **ETH F** interface functionality. This may be necessary in situations where the ETH F, ETH 1, and ETH 2 interfaces are disabled or restricted from accessing the SEL-FLR because of an inadvertent IP configuration settings change. Resetting the Port F functionality will reenable the **ETH F** interface and services (i.e., HTTPS) on that interface.

To reset the **ETH F** interface, while the SEL-FLR is in operation, insert a tool (such as a straightened paper clip) into the pinhole reset (see *Figure 5.23*) and press and hold the recessed button for at least 5 seconds.

Factory Reset

If the login credentials for all administrator and user manager accounts are lost, you must perform a factory-default reset of the SEL-FLR by using the pinhole reset option.

Perform the following steps to reset the SEL-FLR to factory-default settings:

Step 1. Disconnect power to the SEL-FLR.

Step 2. Insert a tool (such as a straightened paper clip) into the pinhole reset and press and hold the recessed button.

Step 3. While still pressing the button, apply power.

Step 4. After 30 seconds, release the button. When the green **ENABLED** LED on the front panel illuminates, the SEL-FLR has reset to factory-default settings and is ready for operation. The **ETH F** interface will be enabled and the IP address of the unit will be 192.168.1.2.

Hardware Watchdog Reset

If the device detects a stalled process, it restarts that process and enters a reset event message in the System Log.

Settings

After a factory-default reset, all settings within the SEL-FLR are reset to their default values.

Front Panel

During a device reset/restart, the front panel temporarily turns off and then back on, after which the SEL-FLR goes through its initialization sequence before becoming operational again.

SECTION 6

Diagnostics

Overview

This section provides information on the alarm contact connections and operation, local and remote Syslog operation, severity thresholds, event acknowledgment, and report fields and filters.

This section includes the following:

SEL-FLR Alarms

The SEL-FLR is equipped with an event reporting system that notifies users to systems alarms or events that occur on the SEL-FLR itself or on linked SEL-FLT devices.

This section includes the following:

Event Reporting System

The SEL-FLR event reporting system is a centralized mechanism that monitors for alerts or alarms on the device and reports these events through various notification subsystems.

The event reporting system provides notification through the Syslog report for all events, and also through the following interfaces based on event severity and device configuration:

- Alarm contact
- Front-panel **ALARM** LED
- Web interface notification

For a list of all the events that trigger Syslog records, see *Appendix C: Syslog*.

Alarm Types

Event reporting interfaces for the alarm contact, front-panel LEDs, and web interface notifications use a two-level method (major or minor) of classifying alarm severity. Syslog reporting also uses a severity classification system ranging from Emergency to Informational.

Major and minor alarms are determined by the Syslog event severity. Event severities of Emergency, Alert, and Critical correspond to a major alarm, while the Error severity corresponds to a minor alarm. Event severities of Warning, Notice, and Informational only generate a Syslog event, and do not trigger a major or minor alarm. A list of all events and their corresponding severity are listed in *Appendix C: Syslog*.

Major Alarms

Major alarms are either an indication that the device has a failed component or that the device experienced a significant change in status, such as a part number change. Major alarms are indicated via various interfaces as follows:

- A local Syslog event is generated
- A remote Syslog event is generated (if configured)
- The alarm contact latches in the alarm condition
- The **ALARM** LED turns on
- The web interface presents a notification and the notification remains active

Many major alarms require operator acknowledgment before the event reporting interface clears the notification. If the condition causing the alarm is not resolved prior to acknowledgment, the alarm notification will reappear after a system restart.

Self-Healing Major Alarms

Some major alarms are self-healing, which means that they are automatically cleared after the condition that created the issue is resolved. For example, if the SEL-FLR detects a flash error, a major alarm condition with event reporting and alarm contact latching occurs. If the system recovers and no other error occurs, the event clears the latched alarm contact and reports that the event condition no longer exists.

Major alarms from SEL-FLT devices can also be self-healing when the SEL-FLT that created the alarm is removed from the whitelist.

Minor Alarms

Minor alarms indicate that a less-significant event has occurred, such as an X.509 certificate expiring. Minor alarms pulse the alarm contact, but unlike major alarms, they do not *latch* the alarm contact. Minor alarms are not reported through web interface notifications.

SEL-FLR Alarm Contact

The SEL-FLR alarm contact is part of the event reporting system that notifies users of an event through the operation of a mechanical Form B contact. The mechanical contact is operated by an output coil. When the coil is de-energized, the contact is closed. This is called a normally closed (NC) contact. The NC symbol and terminal location are shown in *Figure 6.1*.

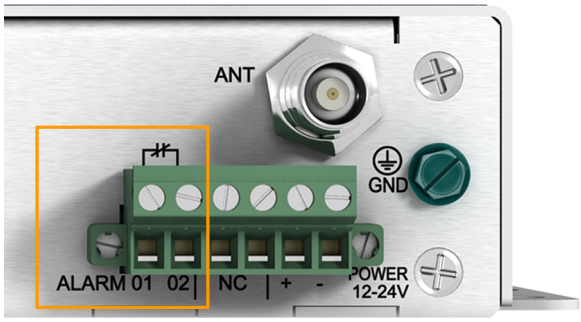


Figure 6.1 SEL-FLR Alarm Contact Pinout

The SEL-FLR energizes the alarm output coil during typical operating conditions (i.e., when the device is energized and in operation). The SEL-FLR de-energizes the alarm output coil after an alarm event. The coil is also de-energized when the SEL-FLR is turned off. The alarm output is a dry contact. See *SEL-FLR Specifications* on page 1.11 for contact electrical ratings.

The alarm contact has two levels of alarm severity: major and minor. The mode of operation defines these two levels.

A major alarm will de-energize the alarm output coil and latch in that mode until it is cleared.

A minor alarm will pulse the contact once by de-energizing the output coil for 1 second and then re-energizing the contact. Any additional minor alarms that occur during an active alarm will be ignored.

SEL-FLR Front-Panel ALARM LED

The **ALARM** LED on the front panel, shown in *Figure 6.2*, illuminates (red) when the device is energized and in an alarm condition (i.e., when the alarm coil is de-energized). The **ALARM** LED pulses for minor alarms and latches for major alarms. Major alarms are cleared when the alarm notification is acknowledged or if the alarm event ceases to occur.

Figure 6.2 Front-Panel ALARM LED

Acknowledging Major Alarms

The web interface allows you to acknowledge a major event by clearing the corresponding alarm. Access the alarm notifications by navigating to **Diagnostics > Alarms** on the SEL-FLR web interface, as shown in *Figure 6.3*.

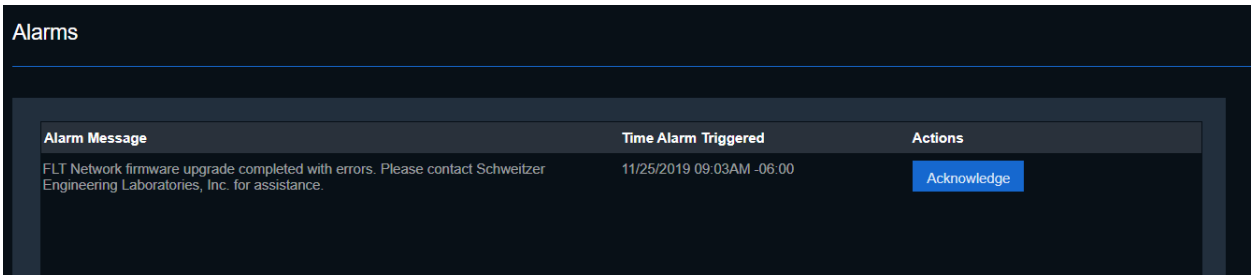


Figure 6.3 Alarm Notifications

Each major alarm must be acknowledged individually. If there are multiple events, they *all* must be acknowledged to clear the corresponding front-panel **ALARM** LED and alarm contact indications.

Dashboard

The Alarm LED on the dashboard replicates the front-panel alarm indicator and illuminates (red) when the device is in an alarm condition (alarm coil de-energized).

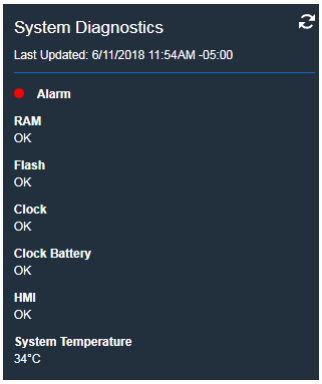


Figure 6.4 Alarm Dashboard LED

Syslog Reporting

The SEL-FLR Syslog reporting is part of the event reporting system that provides notifications through two mechanisms: a local Syslog report and formatted network message traffic.

This section includes the following:

Syslog Severity

The Syslog Protocol includes a Severity field with predefined values representing increasing or decreasing levels of event severity. The following are the values used by the SEL-FLT and SEL-FLR (in order of priority from highest to lowest):

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational

The Syslog settings allow lower-priority messages to be filtered out based on a threshold setting. Setting this threshold to a higher priority filters out all messages with a priority less than the one you have selected (i.e., the SEL-FLR will only send messages with the selected priority or higher). This filtering occurs at the time of the event, so changing the threshold only affects future messages, not preexisting ones. A higher threshold reduces the number of events the SEL-FLR sends to the remote Syslog destinations. This can result in traffic loads being reduced, but it can also cause the loss of key event notifications.

You can set the threshold independently for each remote Syslog destination through the use of the remote Syslog settings.

Local Syslog Reporting

The SEL-FLT and SEL-FLR use a format that contains the same information Syslog messages provide as a local reporting method. Access the local Syslog report by navigating to **Diagnostics > Local Syslog Events** on the SEL-FLR web interface, as shown in *Figure 6.5*.

The SEL-FLR stores information from every event locally, including events from joined SEL-FLT devices. The report maintains as many as 20,000 events; when the maximum is reached, each new event overwrites the oldest event record.

The report contains seven fields: six provide information from the event (Timestamp, Tag, ID, Severity, Facility, and Message), and the seventh (Acknowledged) allows you to acknowledge that event.

Newest records are displayed first by default, but you can sort the data by any column or apply a filter as desired.

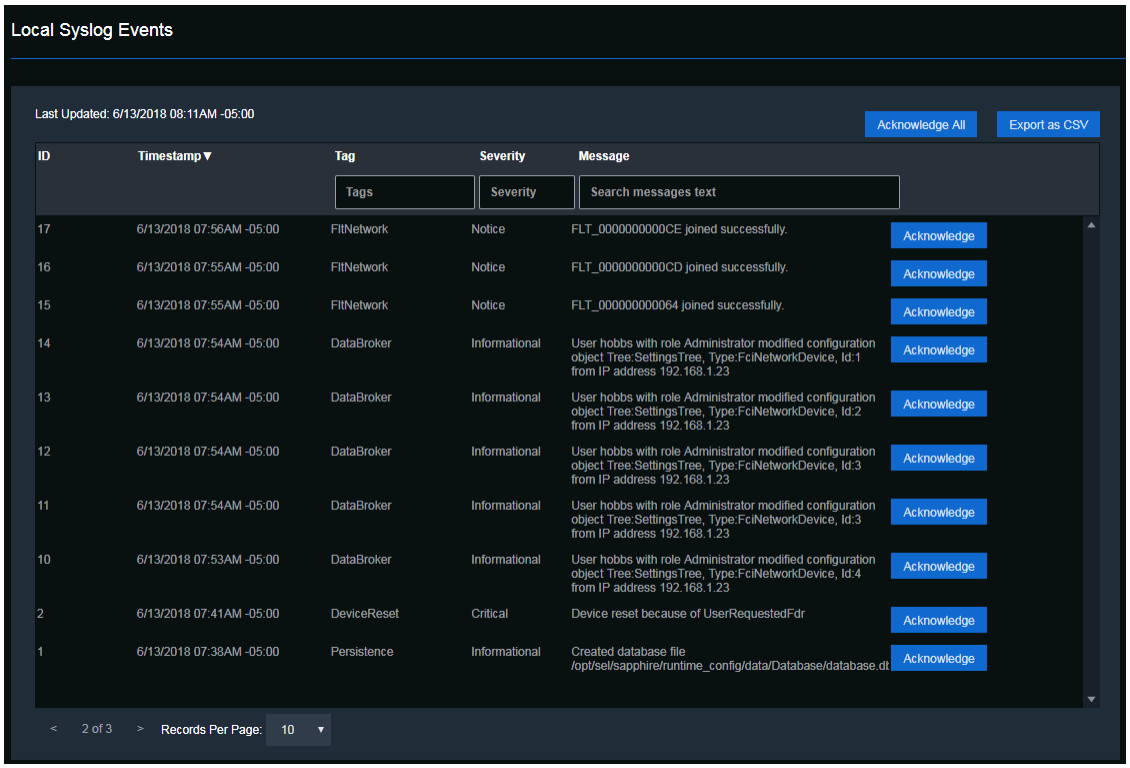


Figure 6.5 Syslog Report

Local Syslog Report Fields

ID represents an index in sequential order for when that event occurred. This number will continue to increment for each event until an SEL-FLR factory-default reset (see *Device Reset* on page 5.18 for details).

Timestamp represents the time the event occurred on the device, using the present device time.

Tag represents the name of the process that generated the event. For example, if the event was generated by an SEL-FLT device or from the integrated radio module, that will be indicated in the Tag field.

Severity represents the level of concern the event represents. The severity levels are representative of the values in the Syslog Protocol (RFC 3164). You cannot adjust the severity levels for the events.

NOTE: Events indicate occurrence of reportable conditions, while the **Severity** field provides a level of concern for each event. The event can be a positive notification, such as achievement of radio link, or a negative notification, such as a link loss.

Message details the action that generated the event. Events that were generated by an SEL-FLT will include the Device Address in the Message field. *Appendix C: Syslog* provides a full list of local Syslog report messages.

Acknowledge Events

After reviewing event records, you should acknowledge them to aid tracking of new event records. Acknowledging an entry does not remove the event, but marks the event as being acknowledged. It is not possible to reverse the acknowledgment of an event.

There are two methods for acknowledging records. The first method is to click the **Acknowledge** button for each desired record. A notification will appear providing indication that the event has been successfully acknowledged. With this method, you must acknowledge each event individually.

NOTE: Using **Acknowledge All** may take several minutes to complete if there is a large number of unacknowledged Syslog messages.

The other method is to click **Acknowledge All**, which acknowledges all unacknowledged records on all pages. Acknowledging all records generates a new event record indicating that all events have been acknowledged.

Acknowledging records generates a new Syslog event record indicating acknowledgment of one or more events.

Exporting Events

Exporting the local Syslog report allows you to download all locally stored event records on the device to a comma-separated-values (CSV) formatted file. Click **Export as CSV** to begin the download of the file **EventLog.csv**. If there is a large number of event records, download time may be significant.

If you open the CSV file directly from Microsoft Excel, the Message column may not display properly. This is because of the automatic default formatting set by Microsoft Excel. To properly view and import the Syslog CSV file by using Excel, follow these steps:

Step 1. Open a blank worksheet in Excel.

Step 2. On the Data tab, in the Get External Data group, click **From Text**.

Step 3. Navigate to the Syslog CSV file and select it, and then click **Import**.

Step 4. In the first step of the Text Import Wizard, configure the settings as follows:

a. Select **Delimited** as the original data type

b. In the File Origin drop-down list, select 65001 : Unicode (UTF-8)

c. Select the **My data has headers** check box

Click **Next** to continue.

Step 5. In the second step of the Text Import Wizard, select the **Comma** check box and clear the **Tab** check box for the delimiters, and then click **Finish**.

Step 6. Choose the location where you want to put the Syslog data in your spreadsheet, and click **OK**.

Your Syslog CSV file should now import and display with the Message field formatted correctly.

Page Filtering

To allow for easy analysis, the Local Syslog report can be filtered by each column. Enter the text to filter by in the filter field at the top of each column. Remove filters by deleting the text from the filter field.

Page Navigation

Local Syslog reporting displays records in a series of pages. The Records Per Page option at the bottom of the page allows you to choose how many records to display on each page (10, 25, 50, and 100).

Remote Syslog Reporting

The SEL-FLR formats and transmits event messages according to the Syslog Protocol defined in RFC 3164. The SEL-FLR can transmit the event messages to multiple different remote Syslog destinations.

Remote Syslog Settings

Set up remote Syslog destinations by navigating to **System > Syslog** on the SEL-FLR web interface, as shown in *Figure 6.6*. You can edit or delete any existing remote Syslog destinations from this page.

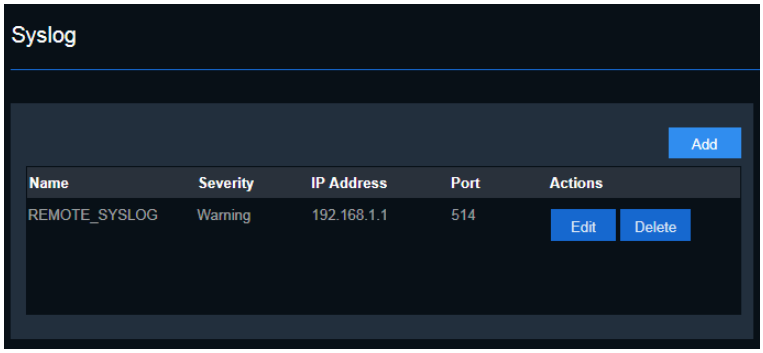


Figure 6.6 Remote Syslog Configuration

To create a new remote Syslog destination, click **Add** to present the dialog box shown in *Figure 6.7*. Set the destination by configuring the settings, as shown in *Table 6.1*, and then click **Create** to apply your changes.

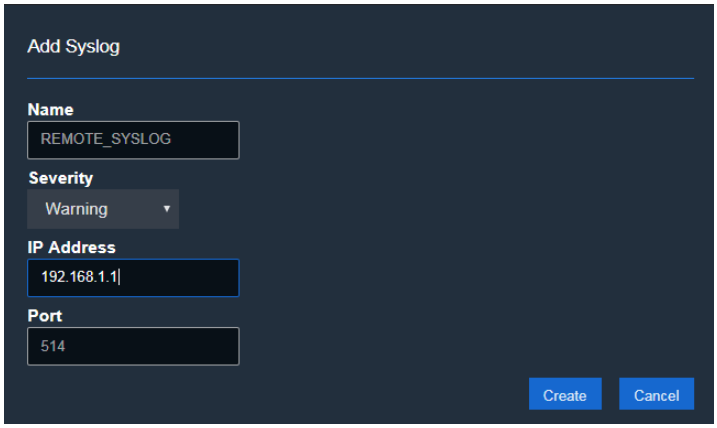


Figure 6.7 Remote Syslog Destinations Setup

Table 6.1 Remote Syslog Destination Settings (Sheet 1 of 2)

Setting Name	Value	Default	Description
Name			A name that is associated with the Syslog destination.
IP Address	Unicast IP Address		The IP address of the Syslog destination.

Table 6.1 Remote Syslog Destination Settings (Sheet 2 of 2)

Setting Name	Value	Default	Description
Port	1–65535	514	The port number for the Syslog destination.
Severity	Emergency Alert Critical Error Warning Notice Informational Debug	Warning	The minimum severity level that an event must have before the SEL-FLR will forward it to this destination.

The remote Syslog destination IP addresses must meet the following requirements:

- All IP addresses defined on the device are IPv4 addresses.
- Destination IP addresses and port combinations must be unique; two or more destinations cannot have the same IP address and port number.
- Destination IP addresses and port numbers cannot be the same as any device Ethernet interface IP address and port number.

This page intentionally left blank

SECTION 7

SEL-FLT Features

Overview

This section provides an overview of basic features and functionality of the SEL-FLT, including the following:

Product Identification

The Device Address (DEV ADDR) and serial number are marked on the SEL-FLT as shown in *Figure 7.1*. The Device Address associates all radio transmissions to a specific device. It is important to keep accurate records of the Device Address for each installed SEL-FLT so you can associate data messages with a particular device.

Figure 7.1 SEL-FLT Device Address and Serial Number Location

Mounting Range

The SEL-FLT will accommodate a range of overhead conductors from 6.4–38.1 mm (0.25–1.50 in). The SEL-FLT installation is identical on either small or large conductors.

CT Lock

The SEL-FLT is secured to the overhead conductor by the spring-loaded clamping bar. The SEL-FLT locking mechanism is designed to secure the clamp around the overhead conductor. This prevents the product from becoming disengaged from the overhead line in the event of severe line whip.

The SEL-FLT locking mechanism is engaged (and disengaged) by moving the hook eye on the back of the product. Pulling the hook eye away from the housing will disengage the lock and allow the core to open and close (as shown in *Figure 7.2*). Releasing the hook eye will engage the locking mechanism when the core returns to the closed position.

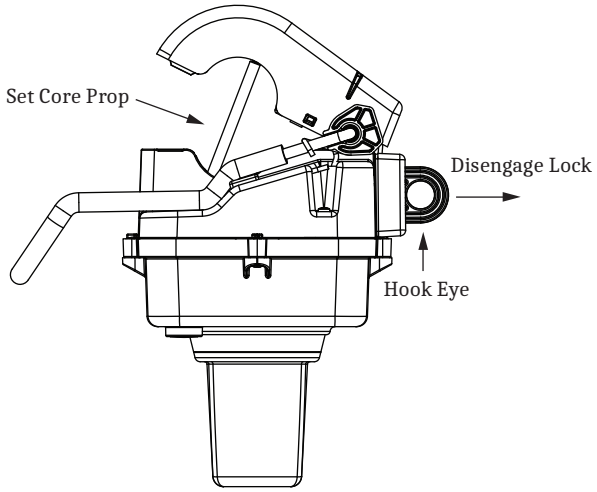


Figure 7.2 Disengage the Locking Mechanism

Magnet Tool Operation

The magnet tool accessory (SEL part number CRSRTT; see *Figure 7.3*) is used to interact with the device, and use of it is required for deployment. Manual resets and radio activation are functions performed using the magnet tool. The local LEDs provide feedback on successful use of the magnet tool.

Remove the shorting bar (shown in *Figure 7.3*) before using the CRSRTT magnet tool. Replace the shorting bar after using the magnet tool.

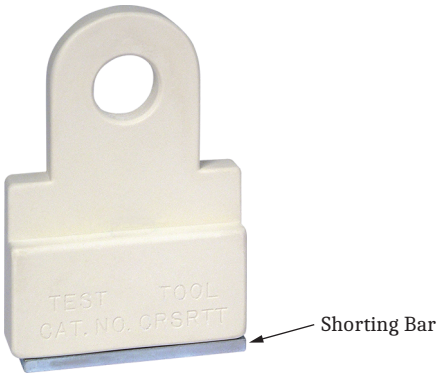


Figure 7.3 CRSRTT Magnet Tool

Short Press

A short press is used to wake the device or manually clear any active LED displays. The SEL-FLT is shipped from the factory in a deep-sleep mode to conserve power. A short press with the magnet tool wakes the device up.

Hold the magnet tool over the **ACTIVATE** label (as shown in *Figure 7.4*) for 3–5 seconds to perform a short press. A single red LED flashes to indicate a short press.

Use a short press to perform the following:

- Wake the device up from deep sleep.
- Clear any active LED displays.
- Start the Test Activate display.

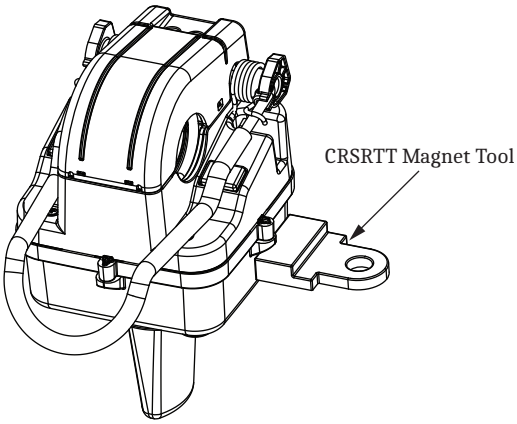


Figure 7.4 Using the CRSRTT Magnet Tool

Long Press

A long press is used to toggle the state (on or off) of the internal radio. The radio in the SEL-FLT is in an off state by default, and it must be activated before being able to send radio transmissions.

Holding the magnet tool over the **ACTIVATE** label (as shown in *Figure 7.4*) for 10–12 seconds will perform a long press, indicated by a single yellow LED flashing rapidly. (A single red LED flashes first to indicate a short press, and then the single yellow LED flashes to indicate the long press.)

Use a long press to perform the following:

- ➤ Turn on the radio (if the radio was in an off state).
- ➤ Start the Radio Enable display (if the radio was in an off state).
- ➤ Turn off the radio (if the radio was in an on state).
- ➤ Start the Radio Disable display (if the radio was in an on state).

Power

Power Harvesting

The SEL-FLT is a line-powered device under normal conditions with a battery backup for extended outages. The SEL-FLT requires a minimum of 3.5 A to support power harvesting. If the current is below 3.5 A, the non-rechargeable batteries will power the device. The SEL-FLT is capable of providing a 15-year service life with greater than 1800 flash hours when line current is at least 3.5 A with a 5-minute Short Update Interval and a 24-hour Long Update Interval.

Low Power Harvesting Alarm

The Low Power Harvest alarm indicates that the SEL-FLT is not harvesting enough power to support the update interval rate. The SEL-FLT will set the Low Harvest Power status when current is below 3.5 A for one complete long update interval period.

The SEL-FLT will clear the Low Harvest Power status after the average current is measured above 3.5 A. This status is indicated on the next update message.

Battery Power

The SEL-FLT uses a backup battery to power the device during extended outages or in low-load applications that do not fully support line powering. The SEL-FLT has a rechargeable battery and a non-rechargeable battery. The battery voltage is sampled every 5 minutes and is reported in millivolts in the Long Update Interval message.

The rechargeable battery is the primary power source and is used during short outages. A full rechargeable battery will power the LED display for longer than 8 hours when no load current is available. The rechargeable battery is charged from power harvesting when available. The rechargeable battery will take approximately 5 days to recharge at 5 A load current and approximately 2.5 days to recharge at 10 A or greater.

The non-rechargeable battery is the secondary power source and is used during extended outages. Once the rechargeable battery has depleted its usable power during an outage, the non-rechargeable battery powers the SEL-FLT and also recharges the rechargeable battery. The non-rechargeable battery provides greater than 1800 flash hours.

Low Rechargeable Battery Alarm

The Low Rechargeable Battery alarm indicates that the rechargeable battery voltage dropped below 3.25 V. The SEL-FLT will send a Low Power Alarm message to indicate the Low Rechargeable Battery status. The SEL-FLT will clear the Low Rechargeable Battery status after the rechargeable battery voltage is measured above 3.30 V.

Critical Rechargeable Battery Alarm (Upcoming Communications Interruption)

NOTE: The SEL-FLT will turn off all functionality while the Critical Rechargeable Battery alarm status is set.

The Critical Rechargeable Battery alarm indicates the rechargeable battery voltage dropped below 3.2 V, and there is an upcoming product outage. Fault and load monitoring functionality is disabled when the rechargeable battery voltage drops below 3.2 V. The SEL-FLT will send one Critically Low Power message to indicate an upcoming communications interruption during which the SEL-FLT will turn off the radio. The SEL-FLT will not send any additional message until the Critical Rechargeable Battery alarm is cleared. The SEL-FLT will not arm or respond to any events until the Critical Rechargeable Battery alarm is cleared.

The SEL-FLT will clear the Critical Rechargeable Battery alarm when the rechargeable battery voltage is measured above 3.3 V. The rechargeable battery will typically be recharged by power harvesting, but can also be recharged from the non-rechargeable battery source. After the Critical Rechargeable Battery alarm is cleared, the SEL-FLT rejoins the network, sends a new Deployment message, and restarts normal operation.

Low Non-Rechargeable Battery Alarm

NOTE: In very cold environments, low ambient temperatures can cause the measured voltage to drop below 3.3 V, resulting in the Low Non-Rechargeable Battery alarm being set. When the ambient temperature rises, the SEL-FLT clears the Low Non-Rechargeable Battery alarm if it was asserted because of environmental conditions rather than as a result of battery capacity.

The Low Non-Rechargeable Battery alarm indicates that the non-rechargeable battery voltage dropped below 3.3 V. The SEL-FLT will send a Low Power Alarm message to indicate the Low Non-Rechargeable Battery status.

The SEL-FLT will clear the Low Non-Rechargeable Battery alarm when the non-rechargeable battery voltage is measured above 3.4 V.

Self-Diagnostics

Flash Error

The SEL-FLT will periodically run system diagnostics on the flash memory. Any diagnostics failures will set the Flash Error alarm status, and the SEL-FLT will transmit an Alarm message.

RAM Error

The SEL-FLT will periodically run system diagnostics on the RAM of the controller. Any diagnostics failures will set the RAM Error alarm status, and the SEL-FLT will transmit an Alarm message.

Event Statistic Reset

The SEL-FLT maintains statistics on various system events for planning and system analysis. Manually resetting the event statistics helps to monitor improvements, maintenance, or changes to the distribution system. The SEL-FLT event statistics are resettable remotely via an over-the-air command from the SEL-FLR, as shown in *Figure 7.5*.

Figure 7.5 Statistics Reset Screen Capture From HMI

SEL-FLT Local Display

This section contains details on the display features and different LED display patterns used by the SEL-FLT.

This section includes the following:

Display Overview

Figure 7.6 SEL-FLT Local Display LEDs

The SEL-FLT is equipped with a local LED display that provides indication of different events and device status. The display consists of six ultra-bright LEDs, three red and three yellow, arranged around the base of the device. The LED display provides 360-degree visibility.

The LED display operates independently of communication with a wireless network, i.e., the LED display still operates even if the SEL-FLT is not paired with an SEL-FLR network.

The LEDs are visible from 50 m (160 ft) during the day and 100 m (330 ft) at night.

The SEL-FLT indicates when the display is active in transmitted messages in the Device Status data field. See *SEL-FLT Message Types and Data* on page 7.12 for details.

When the SEL-FLT measures a low-power condition (e.g., radio transmissions, event detection, and load monitoring), the LED display and other functionality will not operate until sufficient power is available. See *Low Power* on page 7.15 for more information on low-power conditions.

Low Ambient Light Conditions

The SEL-FLT is equipped with a photosensor to detect low ambient light conditions. When the SEL-FLT detects a low ambient light condition, it decreases the intensity of the light output on all LEDs to minimize power consumption.

Extended Outages

During the first 4 hours of an event, the SEL-FLT displays a fast flash pattern to increase visibility. After the first 4 hours, the SEL-FLT displays a slower flash pattern to conserve power. The SEL-FLT remains in the slow flash pattern until either the fault is cleared by the arming requirement or the display time-out is reached.

Event Displays

Permanent Fault Displays

The SEL-FLT has a unique flash pattern used to identify permanent fault events (see *Permanent Fault* on page 8.14 for details on permanent fault detection). During a permanent fault, the SEL-FLT illuminates the red and yellow LEDs in a flash pattern that rotates around the device.

Permanent Fault displays are cleared by the display time-out, arming requirements, or manually through the use of the magnet tool.

Local Event Display

The SEL-FLT has a multipurpose flash pattern used to provide local indication of events. The Local Event display consists of three yellow LEDs illuminated in a flashing pattern. You can configure the SEL-FLT to trigger the Local Event display upon detecting any of the following events:

- Permanent loss of current
- Momentary fault
- Disturbance

Local Event displays are cleared by the display time-out, arming requirements (for permanent loss-of-current events only), manually through the use of the magnet tool, or by a permanent fault event.

If a permanent fault occurs while a Local Event display is active, the Permanent Fault display takes priority over the active Local Event display.

Test Activation Display

Clear any active display by performing a short magnet press (3–5 seconds) with the CRSRTT magnet tool. This triggers the Test Activation display function, which flashes all red and yellow LEDs in sequence followed by just the yellow LEDs. This will repeat three times.

Armed Display

The Armed display provides local indication of when the SEL-FLT has met the configured arming requirements and is ready to detect faults. The Armed display flashes the 3 yellow LEDs 20 times to indicate that the device has armed.

Network Join Display

The Network Join display provides local indication of when the SEL-FLT has successfully connected to an SEL-FLR network and is able to transmit and receive messages. The Network Join display flashes all 3 red LEDs 20 times.

Radio Activation Display

If the radio is presently off, activate the SEL-FLT radio by performing a long magnet press (10–12 seconds) with the CRSRTT magnet tool. This triggers the Radio Activation display, which flashes just one red LED to indicate activation of the radio.

Radio Deactivation Display

If the radio is presently on, deactivate the SEL-FLT radio by performing a long magnet press (10–12 seconds) with the CRSRTT magnet tool. This triggers the Radio Deactivation display, which toggles two red LEDs to indicate deactivation of the radio.

Display Reset

The SEL-FLT turns off any active displays either when the automatic reset requirements are met or when a manual reset is performed.

Magnet Tool Display Reset

You can manually clear the local LED display by performing the test activation procedure (a short magnet press with the CRSRTT magnet tool). The manual test activation clears any active display and initiates the Test Activation Display. See *Testing* on page 9.2 for information on testing the display with the CRSRTT magnet tool.

Display Time-Out

The SEL-FLT shuts off any active display when the display time-out is reached. The Permanent Fault Display Time-Out (T_{PFD}) is the display time-out used for permanent fault events. The Local Event Display Time-Out (T_{DIS}) is the display time-out used for all other events.

System Arming

The SEL-FLT clears the permanent fault display if the arming requirements (e.g., current restoration) are met. See *Section 8: SEL-FLT Event Detection* for details about the arming requirements.

SEL-FLT Load Monitoring

This section contains details on the load monitoring feature of the SEL-FLT device.

This section includes the following:

Load Monitoring

The SEL-FLT monitors and reports accurate load data in near-real time. The SEL-FLT reports load data at both a short and long update interval. The short interval provides near-real-time load updates, whereas the long interval provides load data for an extended duration. These two update interval rates are user-configurable parameters to provide the right amount of data depending on the application. See *SEL-FLT Parameters and Settings* on page 4.28 for details on configuring these parameters.

The SEL-FLT samples current every 5 seconds. The SEL-FLT has a worst-case load measurement accuracy of less than or equal to ±2.5 A + 2% (typically, accuracy is less than ±0.25 A + 1%). Any gap in the core mating surfaces will attribute to load data inaccuracy. Ensure that both core surfaces remain contaminant-free for the best product performance.

The SEL-FLT requires load current greater than the Minimum Current Threshold (I_{MIN}) to sample and report load data. All of the load data fields are reported as 0 A when current is below I_{MIN}.

Short Update Interval Load Data

The Short Update Interval messages provide load data as frequently as every 5 minutes. In each Short Update Interval message, the SEL-FLT reports two rms data points: the average load and the peak measured current.

Average

Each Short Update Interval message contains an average load measurement data point reported in amperes (rms). This value is the average of all sampled load data over the Short Update Interval (T_{SUI}).

Peak

Each Short Update Interval message contains a peak load measurement data point reported in amperes (rms). This value is the greatest load data point taken over the Short Update Interval (T_{SUI}). The SEL-FLT will average three consecutive load samples and report the highest load value (i.e., average over a 15-second interval).

Long Update Interval Load Data

The Long Update Interval messages provide load data over a longer period of time (24 hours by default) than the Short Update Interval. In each Long Update Interval message, the SEL-FLT reports two data points: the average load and the peak measured current.

Average

Each Long Update Interval message contains an average load measurement data point reported in amperes (rms). This value is the average of all sampled load data over the Long Update Interval (T_{LUI}).

Peak

The SEL-FLT reports a peak load data point for the highest measured load current sample over the long update interval. The peak load data help with planning purposes to identify and monitor areas of stress on the system. A rolling average is used to determine the highest measured load current sample over the Long Update Interval. The SEL-FLT uses the Load Peak Window (T_{PEK}) parameter to determine the size of the rolling average.

The SEL-FLT calculates a rolling average by using all of the measurements taken over the T_{PEK} period. *Figure 7.7* shows an example of the rolling average response as a function of the unit input current. This example uses a sample rate of 30 seconds and a window of 1:30 minutes.

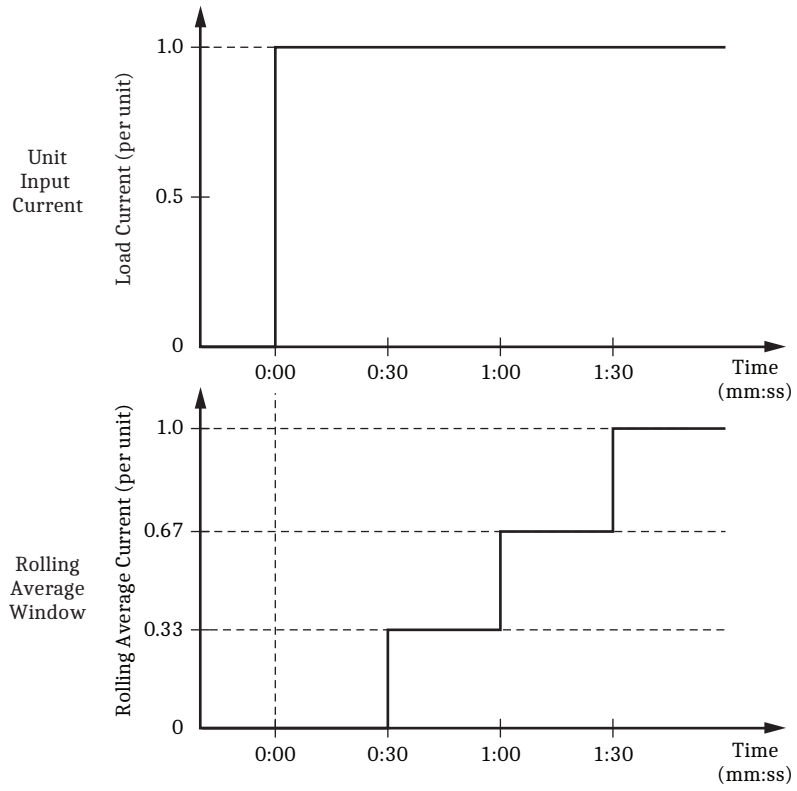


Figure 7.7 Response of Rolling Average to a Step Input

Time = 0:00

Presume that T_{PEK} is configured for 1:30 minutes, and the load current has been zero for at least three measurements (at –1:00, –0:30, and 0:00) before Time = 0:00. The three 30-second intervals in the sliding time window at Time = 0:00 each have a measurement equal to zero.

Rolling average current at Time = 0:00 = $\frac{0.0}{3}$ = 0.0 per unit.

Time = 0:30

The three 30-second intervals in the sliding time window at Time = 0:30 each correspond to the 30-second measurements in *Table 7.1*.

Table 7.1 Rolling Average Peak Load Example, Time = 0:30

Time 0:30	Corresponding 30-Second Intervals
0.0 per unit	–0:30
0.0 per unit	0:00
1.0 per unit	0:30
1.0 per unit	

Rolling average current at Time = 0:30 = $\frac{1.0}{3}$ = 0.33 per unit.

Time = 1:00

The three 30-second intervals in the sliding time window at Time = 1:00 each correspond to the 30-second measurements in *Table 7.2*.

Table 7.2 Rolling Average Peak Load Example, Time = 1:00

Time 1:00	Corresponding 30-Second Intervals
0.0 per unit	0:00
1.0 per unit	0:30
1.0 per unit	1:00
2.0 per unit	

Rolling average current at Time = 1:00 = $\frac{2.0}{3}$ = 0.67 per unit.

Time = 1:30

The three 30-second intervals in the sliding time window at Time = 1:30 each correspond to the 30-second measurements in *Table 7.3*.

Table 7.3 Rolling Average Peak Load Example, Time = 1:30

Time 1:30	Corresponding 30-Second Intervals
1.0 per unit	0:30
1.0 per unit	1:00
1.0 per unit	1:30
3.0 per unit	

Rolling average current at Time = 1:30 = $\frac{3.0}{3}$ = 1.00 per unit.

SEL-FLT Message Types and Data

The SEL-FLT generates three classes of messages: periodic, exception, and alarm. Periodic messages occur at a predefined interval and contain device statistics and load data. Exception messages occur following a system event to indicate a change in the device state. Alarm messages provide notification of critical alerts. The SEL-FLT allows for enabling or disabling message types to control the type and amount of data being reported.

This section includes the following:

Message Types

The SEL-FLR allows for setting which message types are sent by each SEL-FLT on the system to control the types and amount of data being reported. See *SEL-FLT Parameters and Settings* on page 4.28 for details on configuring which messages are transmitted.

Periodic

Periodic messages are time-driven updates. Each periodic message is transmitted at a user-defined interval.

Long Update Interval Message

The SEL-FLT generates a periodic Long Update Interval message at every Long Update Interval (T_{LUI}). The Long Update Interval message occurs at a slower rate than the Short Update Interval message, but contains more data about the device and system.

The default T_{LUI} setting is 24 hours, and Long Update Interval messages are enabled by default.

The Long Update Interval message includes the following Message Data fields:

- Battery voltage of non-rechargeable cell (V)
- Long Update Average Load Current (amperes)
- Long Update Peak Load Current (amperes)
- Device status
- Event statistics

Short Update Interval Message

The SEL-FLT generates a periodic Short Update Interval message at every Short Update Interval (T_{SUI}). The Short Update Interval message occurs at a faster rate than the Long Update Interval message to provide more-frequent load data. Near-real-time load data are ideal for load monitoring and system planning applications.

The default T_{SUI} setting is 1 hour, and Short Update Interval messages are enabled by default.

The T_{SUI} setting automatically defaults to 1 hour when current is measured below 3 A for one Long Update Interval to conserve power by reducing radio transmissions.

The Short Update Interval message includes the following Message Data fields:

- Short Update Average Load Current (amperes)
- Short Update Peak Load Current (amperes)
- Device status

Exception

Exception messages are event-driven messages that provide notification of that event.

Deployment Message

The SEL-FLT sends a Deployment message either to indicate that the device has joined a network after initially activating the radio with the magnet tool or after a successful firmware upgrade.

The Deployment message includes the following Message Data fields:

- Firmware version
- Battery voltage of non-rechargeable cell (V)
- Device status
- Event statistics

Fault Stimulus Message

The SEL-FLT generates a Fault Stimulus message after detecting a fault stimulus event. See *SEL-FLT Fault Detection* on page 8.7 for details on the detection of different fault types.

Fault Stimulus messages are disabled by default.

The Fault Stimulus message includes the following Message Data fields:

- Device status
- Fault magnitude (amperes)

Permanent Fault Message

The SEL-FLT generates a Permanent Fault message after detecting a permanent fault event. See *SEL-FLT Fault Detection* on page 8.7 for details on the detection of different fault types.

Permanent Fault messages are enabled by default.

The Permanent Fault message includes the following Message Data fields:

- Device status
- Fault magnitude (amperes)

Momentary Fault Message

The SEL-FLT generates a Momentary Fault message after detecting a momentary fault event. See *SEL-FLT Fault Detection* on page 8.7 for details on detection of different fault types.

Momentary Fault messages are disabled by default.

The Momentary Fault message includes the following Message Data fields:

- Device status
- Fault magnitude (amperes)

Disturbance Message

The SEL-FLT generates a Disturbance message after detecting a disturbance event. See *SEL-FLT Fault Detection* on page 8.7 for details on detection of different fault types.

Disturbance messages are disabled by default.

The Disturbance message includes the following Message Data fields:

- Device status
- Fault magnitude (amperes)

Permanent Loss-of-Current Message

The SEL-FLT generates a Permanent Loss-of-Current message after detecting a permanent loss-of-current event. See *SEL-FLT Outage Detection* on page 8.3 for details on detection of different outage types.

Permanent Loss-of-Current messages are disabled by default.

The Permanent Loss-of-Current message includes the following Message Data field:

- Device status

Momentary Loss-of-Current Message

The SEL-FLT generates a Momentary Loss-of-Current message after detecting a momentary loss-of-current event. See *SEL-FLT Outage Detection* on page 8.3 for details on detection of different outage types.

Momentary Loss-of-Current messages are disabled by default.

The Momentary Loss-of-Current message includes the following Message Data field:

- Device status

Restoration Message

The SEL-FLT generates a Restoration message after the device arms and is ready to detect events. See *Section 8: SEL-FLT Event Detection* for details on arming requirements.

Restoration messages are enabled by default.

The Restoration message includes the following Message Data field:

- Device status

Alarm

Alarm messages provide alerts to critical device problems.

Coordination Alarm

The SEL-FLT generates a Coordination Alarm message when the device detects a coordination alarm event. See *Coordination Alarm* on page 8.16 for details. The SEL-FLT will not arm or detect events while a Coordination alarm is set. The SEL-FLT will only send one Coordination Alarm message per event.

The Coordination Alarm message includes the following Message Data field:

- Device status

Low Power

The SEL-FLT generates a Low Power message to indicate low or critically low power from any of the SEL-FLT power sources. A Low Power message can result from a low non-rechargeable battery, a low rechargeable battery, or low harvested power.

There are two types of Low Power messages: low and critically low. Low Power messages indicate power sources below normal levels. Critically Low Power messages indicate the rechargeable battery has insufficient power to continue operating. The SEL-FLT will send one Critically Low Power message to indicate an upcoming outage. After sending the Critically Low Power message, the device will power off the radio and other functionality until sufficient power is available. See *Battery Power* on page 7.4 for more information on the SEL-FLT behavior in critically low power conditions.

The Low Power message includes the following data:

- Device status
- Battery voltage (V)
- Upcoming outage status

Memory Error

The SEL-FLT generates a Memory Error message after failing a RAM or flash memory self-diagnostic test. See *Self-Diagnostics* on page 7.5 for details on the different types of memory failures.

The Memory Error message includes the following Message Data field:

- Device status

Message Data

Different message types will contain different data fields. Limiting the transmitted data to only new, updated information will reduce network traffic and maximize efficiency.

Device Status

Device status data contain the following general information about the state of the SEL-FLT device:

- Message type
- Fault status
- Outage status
- LED display status
- Armed status
- Low Non-Rechargeable Battery Alarm
- Low Rechargeable Battery Alarm
- Critical Rechargeable Battery Alarm (Upcoming Outage)
- Low Power Harvesting Alarm
- RAM Error Alarm
- Flash Error Alarm

Event Statistics

Event statistics contain counters for the different system events and are stored from deployment or after a user-reset of event statics.

The Event Statistics contain the following counters:

- Fault Stimulus Counter
- Permanent Fault Counter
- Momentary Fault Counter
- Disturbance Counter
- Permanent Loss-of-Current Counter
- Momentary Loss-of-Current Counter
- Coordination Alarm Counter
- Display Total Time
- Display Time Greater Than 8 Hours

This page intentionally left blank

SECTION 8

SEL-FLT Event Detection

Overview

This section explains the system conditions required for the SEL-FLT to arm, as well as outage detection and fault detection behavior.

This section includes the following:

SEL-FLT Device Arming

This section contains details on the requirements and process of arming the SEL-FLT device. The device will arm when it detects a power restoration (e.g., load current). Once armed, the SEL-FLT will be able to detect system fault and outage events.

This section includes the following:

Device Arming

The SEL-FLT must be armed prior to a system event (fault or outage) to detect and report that event. The SEL-FLT arms when it detects sustained load current. This is defined by measuring load current that is both greater than the Current Arming Level (I_{ARM}) and sustained for longer than the System Arming Period (T_{ARM}). The SEL-FLT starts the T_{ARM} timer upon measuring current greater than the I_{ARM} threshold. If the SEL-FLT detects an outage during the T_{ARM} time period, the device will not arm and the T_{ARM} timer will be reset.

NOTE: The SEL-FLT does not require a connection to a wireless network to arm.

Figure 8.1 shows a sample load current (I_{LOAD}) profile (in rms values) that results in the SEL-FLT arming at the end of the T_{ARM} period. When the device arms, it transmits a Restoration message by default. The local LEDs will also flash the Armed display.

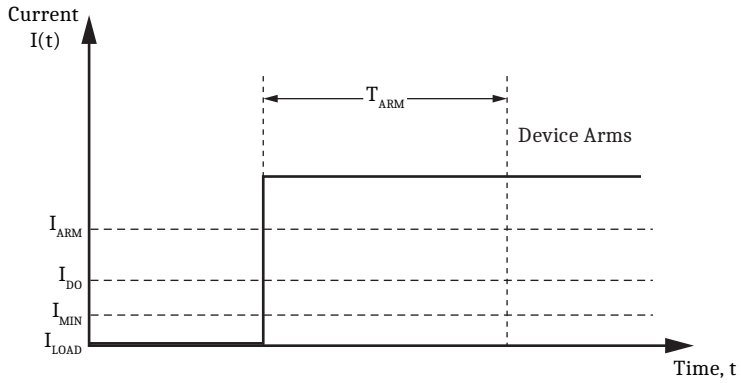


Figure 8.1 Device Arming

NOTE: The SEL-FLT will not arm if a Coordination alarm is set.

The SEL-FLT must measure load current below the highest trip threshold to arm. If the load current is greater than the highest configured trip threshold, a Coordination alarm is set and the device will not arm. See *Coordination Alarm* on page 8.16 for additional details.

While arming, the device will autorange to a trip threshold that is appropriate for the measured load current (see *AutoRANGER Trip Logic* on page 8.8 for details).

The SEL-FLT will not trip or report a fault if the system energization inrush current exceeds the trip threshold during the T_{ARM} period. This behavior is due to the inrush restraint feature that prevents false tripping from inrush current. See *Inrush Restraint* on page 8.6 for more information.

Figure 8.2 shows a sample load current (I_{LOAD}) profile (in rms) where the load current is measured above the I_{ARM} threshold, but not sustained for the full duration of the T_{ARM} time period. Therefore, the SEL-FLT will not arm at the end of the T_{ARM} period.

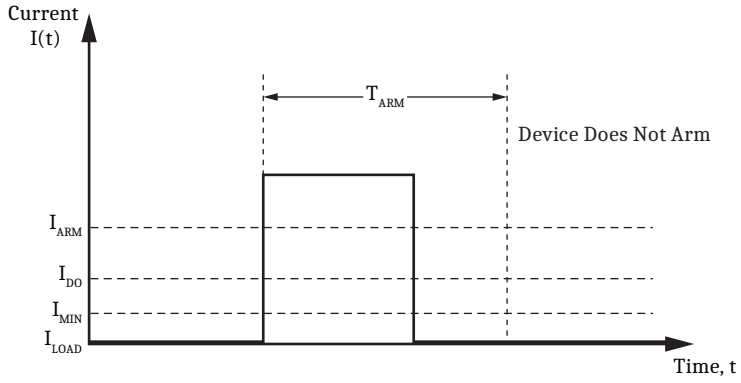


Figure 8.2 Device Does Not Arm

For momentary events (momentary faults, momentary loss of current, disturbance, or load pickup) the device will rearm at the end of the Fault Time-Out (T_{FLT}) or Loss-of-Current Time-Out (T_{LOC}).

Arming Requirements

Current Arming Threshold

The minimum current threshold required to arm the SEL-FLT is defined by the configurable Current Arming Level (I_{ARM}) parameter. The SEL-FLT must measure load current (in rms) greater than the I_{ARM} threshold to start the arming process. See *Current Arming Threshold (I_{ARM})* on page 4.29 for details on configuring I_{ARM}.

System Arming Time

The duration for which the SEL-FLT must detect current above the I_{ARM} threshold is defined by the configurable System Arming Period (T_{ARM}) parameter. The SEL-FLT will start the T_{ARM} timer upon measuring current greater than the I_{ARM} threshold. The T_{ARM} timer will reset if the current drops below I_{DO} or I_{MIN} during the arming period. See *System Arming Period (T_{ARM})* on page 4.29 for details on configuring T_{ARM}.

Arming Hold-Off

The Arming Hold-Off feature will prevent the SEL-FLT from arming for a user-configurable amount of time. This feature is enabled using the Enable Arming Hold-Off parameter, and the time period is configured using the Arming Hold-Off Period (T_{HO}). See *Arming Hold-Off Period (T_{HO})* on page 4.29 for details on configuring T_{HO}.

When this feature is enabled, the SEL-FLT will start the Arming Hold-Off Period after detecting a permanent fault or outage event. The device will not arm during this hold-off period even if power is restored. At the end of the Arming Hold-Off Period, the SEL-FLT will begin checking for the arming requirements (e.g., load current).

SEL-FLT Outage Detection

This section contains details on the outage detection feature of the SEL-FLT device.

This section includes the following:

Current Outage Detection

NOTE: If the SEL-FLT is not armed prior to a fault event, it will not detect or report that event.

The SEL-FLT registers an outage event when a loss of current is detected. The SEL-FLT is equipped with two methods for detecting loss-of-current outages: a fast dropout Minimum Current Threshold (I_{MIN}), and a slow, user-configurable dropout Current Dropout Threshold (I_{DO}). The I_{DO} threshold is used when the system backfeed current may prevent the fast I_{MIN} threshold from detecting an event. Both the I_{DO} and I_{MIN} thresholds are active, meaning either will trigger an outage event.

The SEL-FLT must be armed prior to a system event (fault or outage) to detect and report that event. See *Section 8: SEL-FLT Event Detection* for details about the arming requirements. The SEL-FLT will unarm immediately after detecting an outage.

Minimum Current Threshold (I_{MIN})

The Minimum Current Threshold (I_{MIN}) is a fixed, hardware-defined, fast dropout threshold. The I_{MIN} threshold level and response time are not user-configurable. The I_{MIN} threshold ranges from 1 A to 3 A. The I_{MIN} threshold has a typical response time of 75 ms. When current drops below I_{MIN} for longer than 75 ms, the SEL-FLT registers a loss-of-current event, as shown in *Figure 8.3*. After registering a loss-of-current event, the SEL-FLT starts the Loss-of-Current Time-Out (T_{LOC}) timer and enters an inrush restraint state.

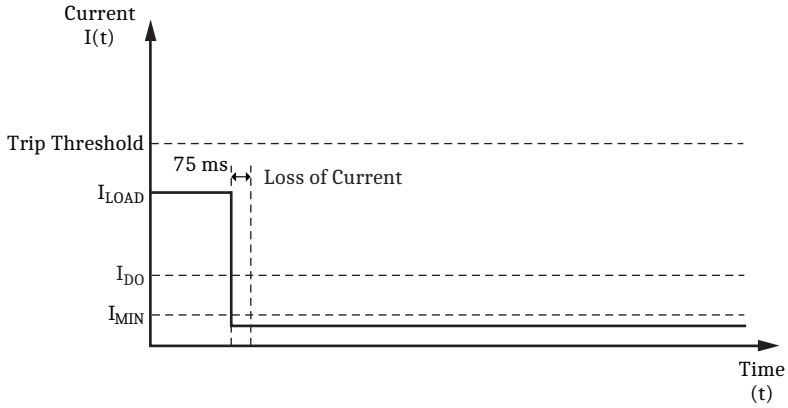


Figure 8.3 Outage Detection—Fast Dropout

Current Dropout Threshold (I_{DO})

The Current Dropout Threshold (I_{DO}) is a user-configurable dropout threshold. The I_{DO} threshold has a typical response time of 30 seconds, which is much slower than the I_{MIN} threshold. When current drops below I_{DO} for longer than 30 seconds, the SEL-FLT registers a loss-of-current event, as shown in *Figure 8.4*. After registering a loss-of-current event, the SEL-FLT starts the Loss-of-Current Time-Out (T_{LOC}) timer and enters an inrush restraint state. See *Current Dropout Threshold (I_{DO})* on page 4.35 for information about changing the I_{DO} threshold.

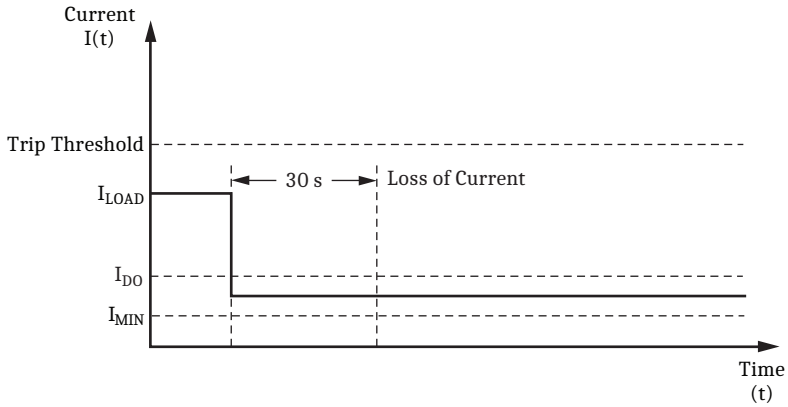


Figure 8.4 Outage Detection—Slow Dropout

Outage Event Types

After detecting an outage event, the SEL-FLT determines the type of outage event by checking for load current at the end of the Loss-of-Current Time-Out (T_{LOC}) period. The Loss-of-Current Time-Out parameter is 5 minutes by default and is user-configurable. See *Loss-of-Current Time-Out (T_{LOC})* on page 4.35 for details on configuring the T_{LOC} setting.

Permanent Loss of Current

To register a permanent loss-of-current event, the SEL-FLT must detect a sustained outage at the end of the Loss-of-Current Time-Out (T_{LOC}) timer.

After detecting an outage, the SEL-FLT starts the T_{LOC} timer. The SEL-FLT checks if the load current is present at the end of the T_{LOC} timer. If there is no load current (indicating a sustained outage), the SEL-FLT registers a permanent loss-of-current event. *Figure 8.5* shows a sample load current (I_{LOAD}) profile (in root-mean-square [rms]) that results in the SEL-FLT registering a permanent loss-of-current event.

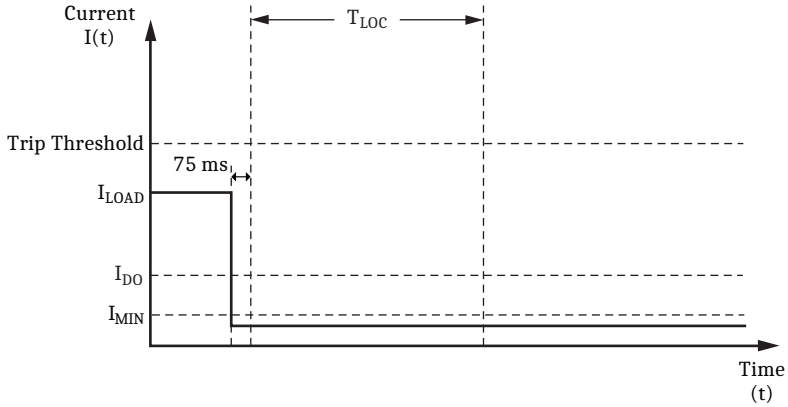


Figure 8.5 Permanent Loss of Current

After detecting a permanent loss-of-current event, the SEL-FLT increments the Permanent Loss-of-Current counter in the event statistics. The SEL-FLT then generates an exception Permanent Loss-of-Current message (when enabled) to report the event. The device also starts the local LED flash pattern when configured to display the event. The SEL-FLT is unarmed at the end of the T_{LOC} timer after detecting a permanent loss-of-current event and begins checking system conditions for a current restoration.

Momentary Loss of Current

To register a momentary loss-of-current event, the SEL-FLT must detect a successful power restoration before the end of the Loss-of-Current Time-Out (T_{LOC}) timer.

After detecting an outage, the SEL-FLT will start the T_{LOC} timer. The SEL-FLT must detect a successful power restoration (indicated by current measured above the I_{ARM} threshold). If the load current is detected at the end of the T_{LOC} timer, the SEL-FLT registers a momentary loss-of-current event. *Figure 8.6* shows a sample load current (I_{LOAD}) profile (in rms) that results in the SEL-FLT registering a momentary loss-of-current event.

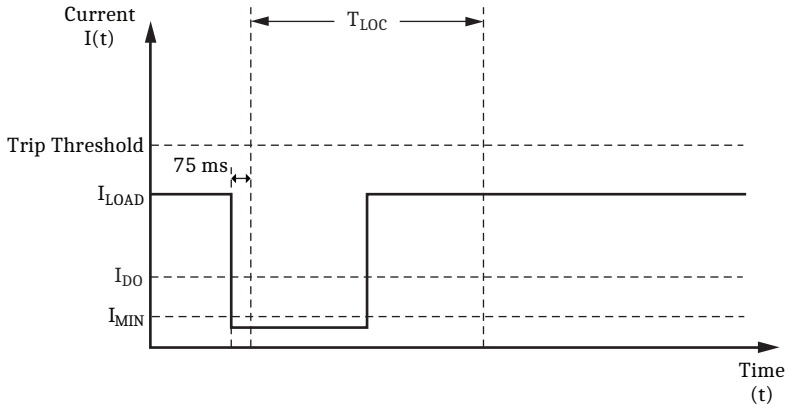


Figure 8.6 Momentary Loss of Current

After detecting a momentary loss-of-current event, the SEL-FLT increments the Momentary Loss-of-Current counter in the event statistics. The SEL-FLT then generates an exception Momentary Loss-of-Current message (when enabled) to report the event. After detecting a momentary loss-of-current event, the SEL-FLT arms and sets the active trip threshold based on the load current measured at the end of the T_{LOC} timer.

Inrush Restraint

Inrush restraint is a feature that prevents the SEL-FLT from misoperating based on system energization. A fault indicator applied on a circuit that uses a reclosing scheme should be able to distinguish between fault events and system energization inrush currents occurring during reclose attempts. Otherwise, the reclosing operations could falsely trip indicators installed on non-faulted line sections.

When an outage is detected, the SEL-FLT enters into inrush restraint mode. While inrush restraint is active, the device will not respond to any events or faults. For permanent outage events and permanent fault events, inrush restraint remains active until power is restored and the arming requirements are met.

Figure 8.7 shows an example of a permanent loss-of-current outage followed by a system restoration some time later. The region labeled *Inrush Restraint Activated* indicates the duration for which inrush restraint is active. The inrush current resulting from system energization may exceed the trip threshold, but the SEL-FLT will not register a fault event while inrush restraint is active. For permanent outages (like the example in *Figure 8.7*), the total duration of inrush restraint is the entire outage duration plus T_{ARM}.

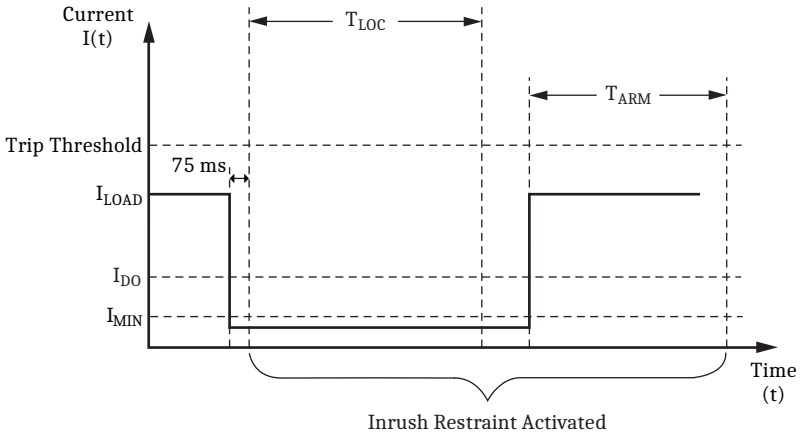


Figure 8.7 Inrush Restraint—Permanent Outage

For momentary events in which power is restored prior to the T_{FLT} or T_{LOC} time-out, inrush restraint will only be active for the duration of the T_{FLT} or T_{LOC} period. At the end of the T_{FLT} or T_{LOC} time-out, the SEL-FLT rearms.

Figure 8.8 shows an example of a momentary loss-of-current event followed by a successful reclose. The region labeled *Inrush Restraint Activated* indicates the duration for which inrush restraint is active.

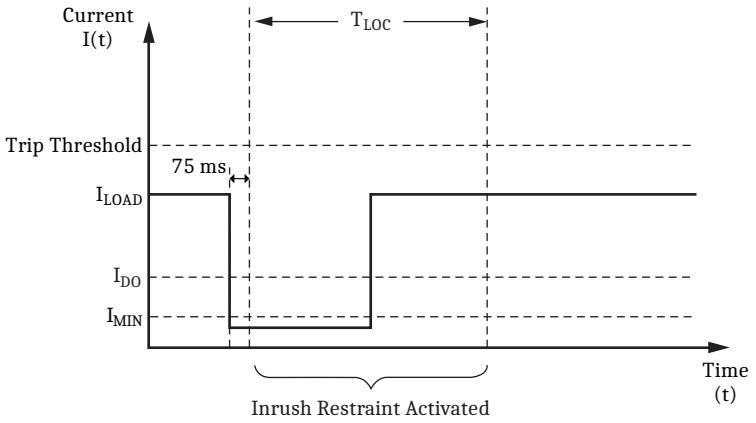


Figure 8.8 Inrush Restraint—Momentary Outage

SEL-FLT Fault Detection

The SEL-FLT uses AutoRANGER trip logic to ensure simple deployment and coordination with a wide variety of loads across an entire distribution system. The SEL-FLT allows for customizing the trip thresholds and delay trip times to optimize performance for specific applications. The SEL-FLT also distinguishes between different fault event types.

This section includes the following:

AutoRANGER Trip Logic

The AutoRANGER trip logic adapts the trip threshold based on the load current for automatic coordination across an entire distribution circuit. The settings for enabling thresholds (Enable AutoRANGE Thresholds), the trip threshold values (AutoRANGE Trip Threshold), and the delay trip times (AutoRANGE Delay Trip) are all configurable through the associated SEL-FLR. See *SEL-FLT Parameters and Settings* on page 4.28 for details on configuring these settings. The highest AutoRANGE trip threshold should always be configured above the maximum load current for the circuit. If the measured load current is greater than the highest configured AutoRANGE trip threshold, a Coordination alarm is set and the device will not arm (see *Coordination Alarm* on page 8.16 for more information).

NOTE: The SEL-FLT will not arm if a Coordination alarm is set.

The SEL-FLT has 10 AutoRANGE trip thresholds enabled by default: 25 A, 50 A, 100 A, 200 A, 400 A, 600 A, 800 A, 1000 A, 1200 A, and 1600 A. The unit automatically selects, or autoranges, to one of these thresholds according to the load current measurements. The SEL-FLT samples the load current every 5 seconds and adjusts the active threshold based on a 30-second rolling average. The active threshold is the lowest current at which the SEL-FLT will trip. Based on the load measurement, the unit either remains at its active trip threshold, ranges up to a higher threshold, or ranges down to a lower threshold. This AutoRANGE feature enables the SEL-FLT to handle variable loads including seasonal and time-of-day fluctuations, simplifying specification, application, and stocking. *Table 8.1* shows the range-up and range-down load current values for each of the default AutoRANGE trip thresholds.

Table 8.1 AutoRANGE Trip Threshold Range-Down and Range-Up Values

Trip Threshold (A)	Load Range-Down Level (A)	Load Range-Up Level (A)
25	N/A	12.50
50	11.25	25
100	22.50	50
200	45	100
400	90	200
600	180	300
800	270	400
1000	360	500
1200	450	600
1600	540	N/A

The SEL-FLT will range up to the next higher trip threshold when the load current exceeds 50 percent of the present trip threshold. For example, at a 100 A trip threshold, the SEL-FLT will range up to the next higher threshold (200 A) when the load current is measured greater than 50 A. The SEL-FLT will only range up one threshold at a time. The SEL-FLT will deactivate trip thresholds below the active trip threshold. For example, if the SEL-FLT has autoranged to a 100 A threshold, the lower 25 A and 50 A thresholds are deactivated, and the device will not trip for currents at 25 A or 50 A. All trip thresholds above the active threshold and their associated trip times will remain active. The SEL-FLT will only range up as high as the highest enabled trip threshold.

The SEL-FLT will range down to the next lower trip threshold when the load current falls to 45 percent of the next lower trip threshold. For example, at a 100 A threshold, the SEL-FLT will range down to the next lower threshold (50 A) when

the load current less than 22.5 A is measured. The SEL-FLT will only range down one threshold at a time. When the SEL-FLT is in the lowest trip threshold (25 A by default), it will not range down because there are no lower trip thresholds.

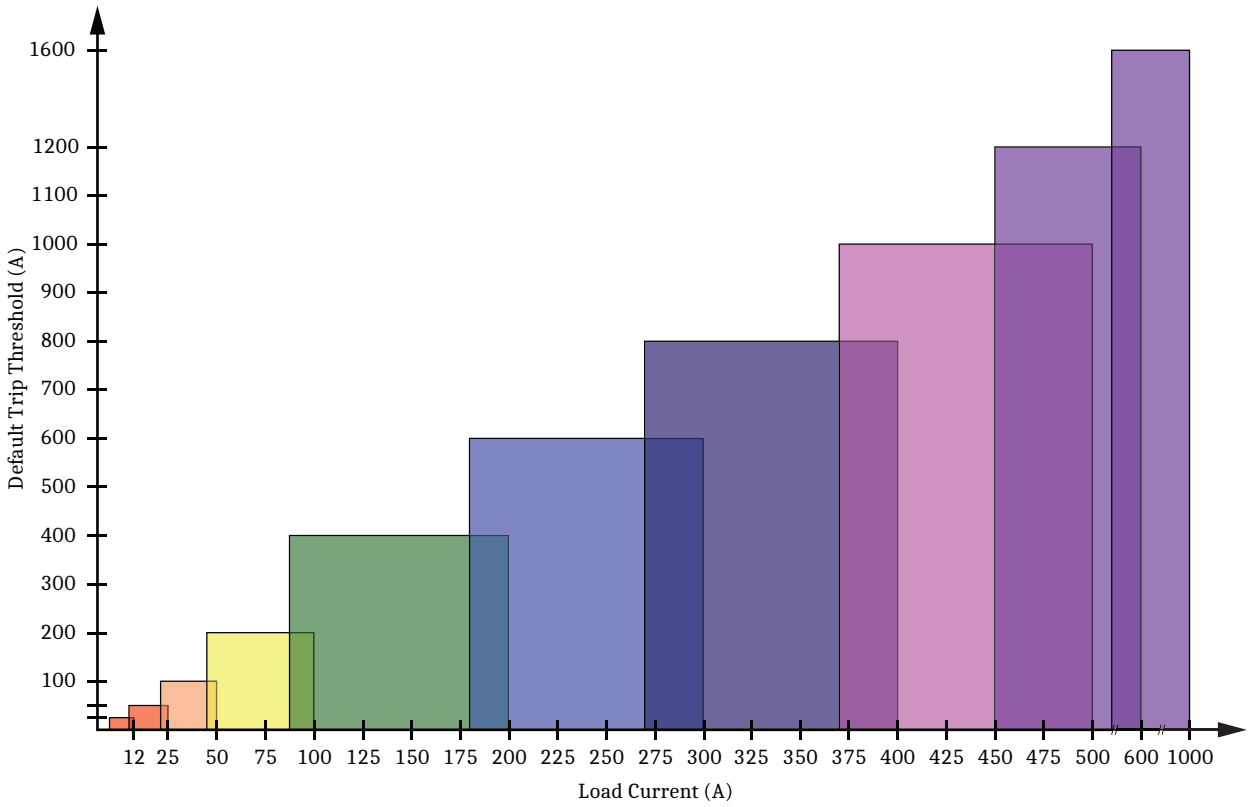


Figure 8.9 Self-Configured Trip Thresholds

The range-up and range-down levels overlap for each trip threshold (regardless of their setting), as shown in *Figure 8.9*. This provides hysteresis to the autoranging algorithm and prevents the SEL-FLT from oscillating between trip thresholds. (If the load current ranges did not overlap, normal fluctuations in the load current would cause the SEL-FLT to oscillate between two trip thresholds.) *Figure 8.10* illustrates how overlapping load current cutoffs for adjacent trip thresholds stabilize the trip threshold and allow the SEL-FLT to select a single trip threshold.

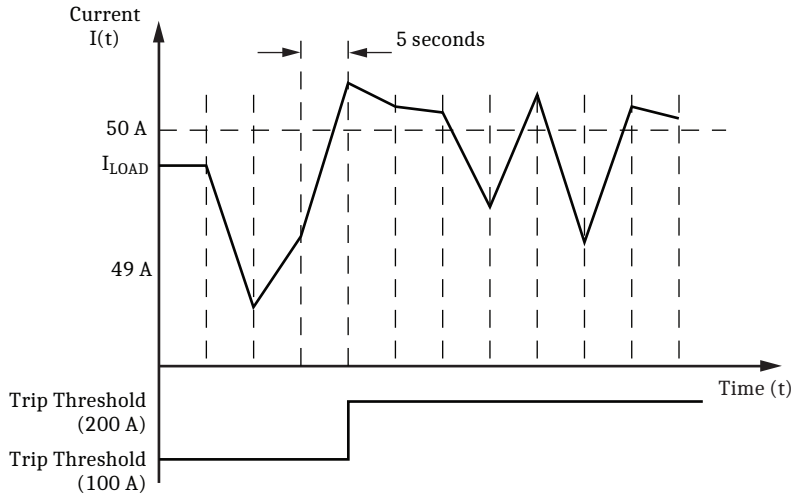


Figure 8.10 Stable Autoranging Algorithm

Fixed Trip Threshold

For applications where the self-adjusting AutoRANGER trip logic is not desired, the SEL-FLT can also operate as a fixed trip threshold device. By disabling all but one of the AutoRANGE trip thresholds, the SEL-FLT will only have one active trip threshold. This trip threshold is the only value the SEL-FLT will trip at; it will not range up or down (see *Enable AutoRANGE Threshold* on page 4.31 for more information).

Use of a fixed trip threshold requires careful coordination with the system protection curve settings (e.g., recloser, relay, fuse, etc.) to ensure the SEL-FLT properly responds to fault events. For proper coordination, configure the SEL-FLT trip threshold above the maximum load current, but below minimum expected fault current. This ensures the SEL-FLT does not trip on load current, and always responds to fault events before the upstream protection clears the fault.

NOTE: The SEL-FLT will not arm if the measured current is greater than the trip threshold.

If the load current is measured above the trip threshold, the SEL-FLT will register a Coordination alarm. The SEL-FLT will not arm if a Coordination alarm is set (see *Coordination Alarm* on page 8.16 for more information).

Trip Response Curve

To properly detect faults, the SEL-FLT must coordinate with the system protection. This requires a faster SEL-FLT trip time than the total clear time of the upstream protection. The SEL-FLT allows for customizing the AutoRANGE Delay Trip settings for each individual AutoRANGE trip threshold. This feature allows you to create customized SEL-FLT trip response curves to coordinate with system protection schemes. See *AutoRANGE Delay Trip* on page 4.32 for more information on setting the AutoRANGE Delay Trip parameter.

The default delay trip for all 10 trip thresholds is three half-cycles (24 ms at 60 Hz). This setting was selected as the default to fit most applications; it ensures that the SEL-FLT detects events before any system protection element operates. However, certain system conditions or various protection schemes can cause the SEL-FLT to respond to faults in a manner other than intended. Applying a customized trip response curve helps prevent the SEL-FLT from falsely indicating fault conditions because of short bursts of high current that might occur normally, but which do not indicate a fault. Applying a customized delay trip curve allows you to set the duration for which fault current must exceed the trip threshold

before the SEL-FLT indicates a fault. The combination of automatic trip threshold selection and a customized delay trip curve allows for optimal coordination of the SEL-FLT into almost any circuit protection scheme.

Figure 8.11 shows the default trip response times for the SEL-FLT. Notice that the default delay trip times of each trip threshold are all equal and provide a faster response time than the system protection curve. This ensures that the SEL-FLT detects events before the upstream protection operates. In some cases, however, this can lead to undesired operations if the system exhibits transient events not registered by the system protection which may not be considered faults.

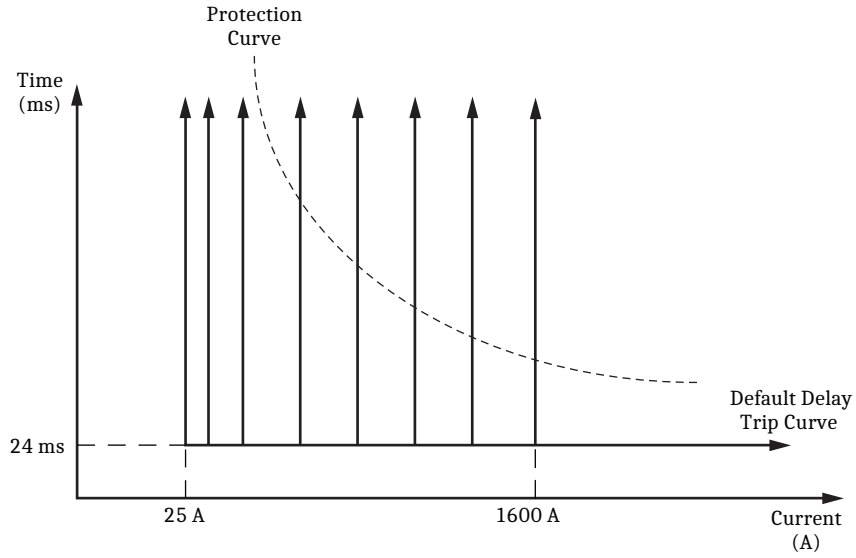


Figure 8.11 Default SEL-FLT Response Curve

Figure 8.12 shows the same protection curve as in *Figure 8.11*, but it includes a coordinated SEL-FLT delay trip curve. The delay trip time of each trip threshold is customized to produce a response curve that coordinates with the protection scheme.

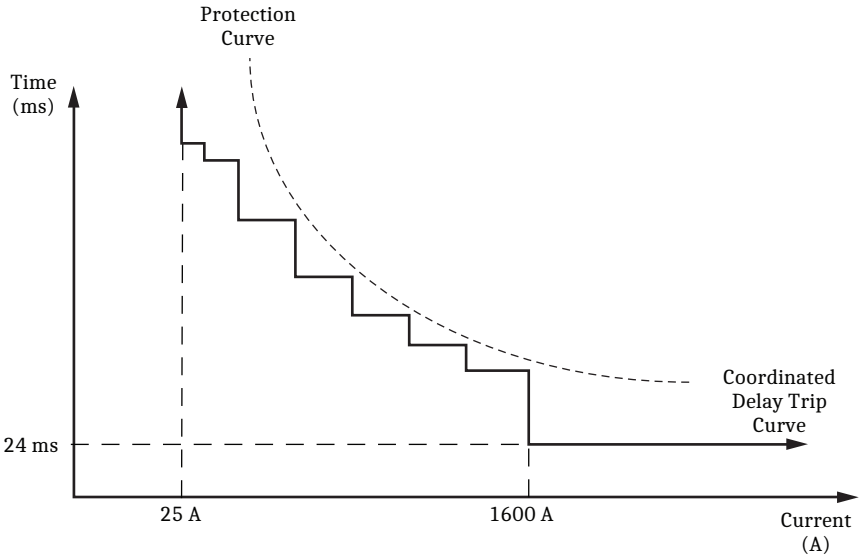


Figure 8.12 Coordinated SEL-FLT Response Curve

Fault Detection

The SEL-FLT must be armed prior to the fault event to detect that event. See *Section 8: SEL-FLT Event Detection* for details on the arming requirements.

The SEL-FLT will detect a fault event when current is measured in excess of the active AutoRANGE trip threshold for longer than the AutoRANGE Delay Trip time. These requirements are configurable using the AutoRANGE Trip Threshold and AutoRANGE Delay Trip settings. See *Fault* on page 4.31 for details on configuring these parameters. To register a fault event, the SEL-FLT must first detect fault current in excess of the active trip threshold. Then, the current must exceed the active trip threshold (or any higher trip threshold) for the defined delay trip. For example, at a 100 A trip threshold with a 3 half-cycle delay trip, current must remain above 100 A for longer than 3 half-cycles (24.9 ms at 60 Hz) to register a fault event, as shown in *Figure 8.13*.

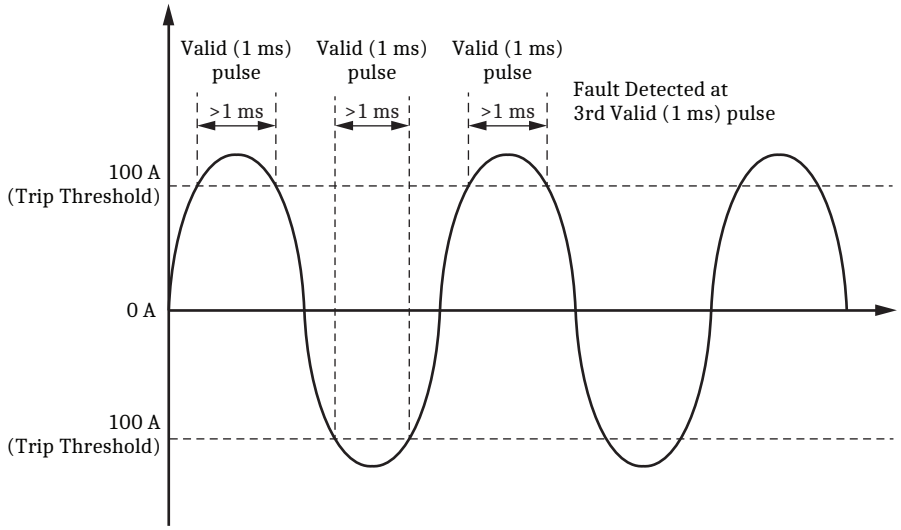


Figure 8.13 Sample Fault Detection

Conditions on the system may cause the fault current of every other half-cycle to not exceed the trip threshold. The SEL-FLT fault detection logic considers each half-cycle of fault current to be continuous if the ac waveform exceeds the trip threshold within 1 cycle of the previous time at which the waveform exceeded the trip threshold (see *Figure 8.14*). If the current does not exceed the trip threshold for at least 1 ms within 1 cycle, the SEL-FLT resets the delay trip counter and the device rearms.

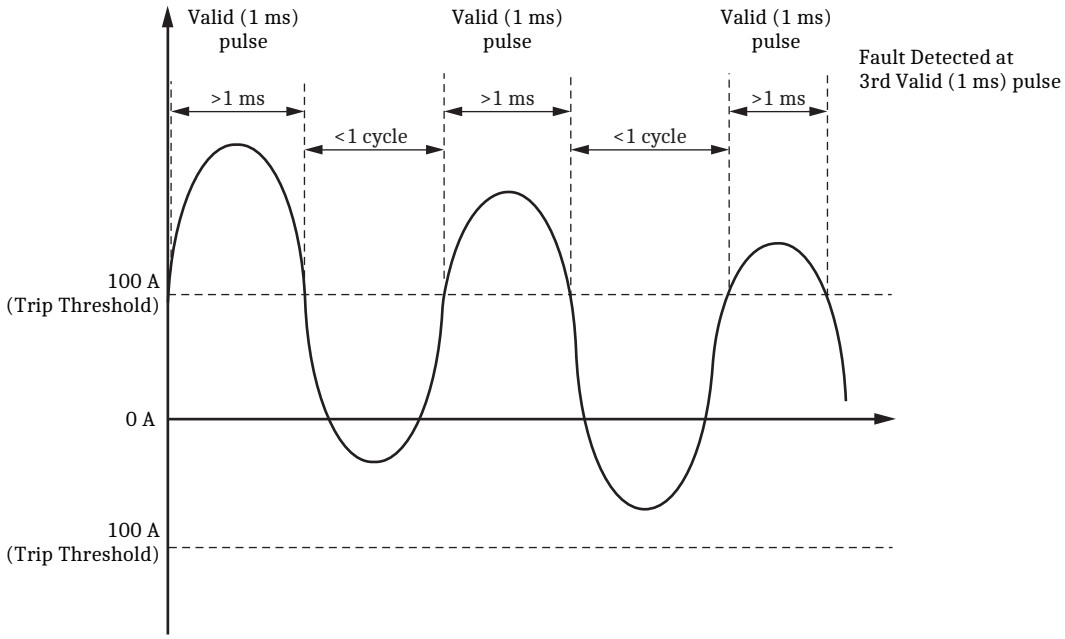


Figure 8.14 Sample Asymmetrical Fault Detection

Fault Event Types

After detecting fault current, the SEL-FLT will determine the type of fault event by checking for load current at the end of the Fault Time-Out (T_{FLT}) period. The Fault Time-Out parameter is 5 minutes by default and is configurable. See *Fault Time-Out (T_{FLT})* on page 4.32 for details on configuring the T_{FLT} setting.

Fault Stimulus

A fault stimulus is the first part of any fault event. A fault stimulus occurs when current exceeds the trip threshold for the delay trip time. *Figure 8.15* shows a sample load current (I_{LOAD}) profile (in rms) that results in the SEL-FLT registering a fault stimulus.

After detecting a Fault Stimulus event, the SEL-FLT will become unarmed and start the Fault Time-Out (T_{FLT}) timer. The SEL-FLT will start the Permanent Fault display local LED flash pattern during the T_{FLT} period. The T_{FLT} timer is used to determine the type of fault event. The SEL-FLT will increment the Fault Stimulus counter in the event statistics. The SEL-FLT then generates an exception Fault Stimulus message (when enabled) to report the event.

A Fault Stimulus is not registered if the current exceeds the threshold but does not persist for the duration of the delay trip time. The SEL-FLT will rearm after not detecting fault current above the trip threshold for 20 ms.

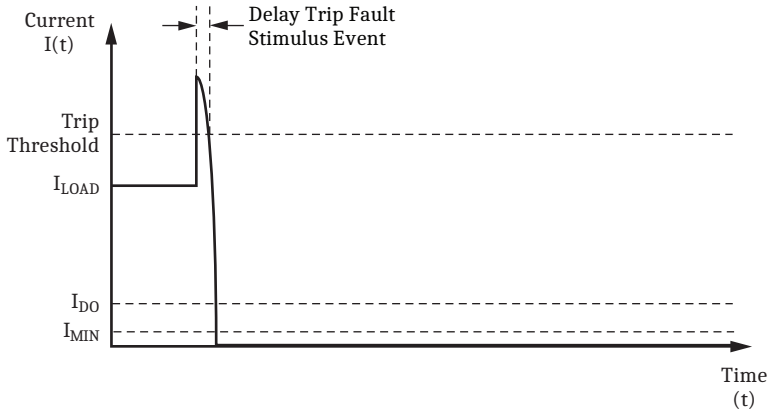


Figure 8.15 Fault Stimulus Event

Permanent Fault

To register a permanent fault event, the SEL-FLT must first detect a fault stimulus followed by an outage at the end of the Fault Time-Out (T_{FLT}) period.

After detecting a fault stimulus, the SEL-FLT will start the T_{FLT} timer. The SEL-FLT will check if the load current is present at the end of the T_{FLT} period. If there is no load current (which indicates an outage), the SEL-FLT will register a permanent fault event. *Figure 8.16* shows a sample load current (I_{LOAD}) profile (in rms) that results in the SEL-FLT registering a permanent fault event.

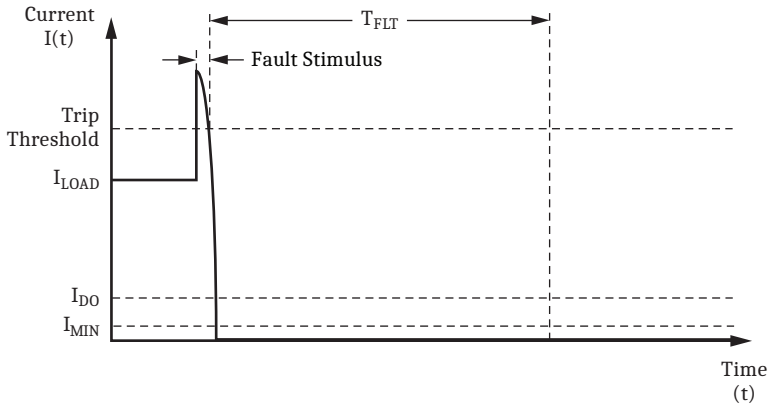


Figure 8.16 Permanent Fault

After detecting a permanent fault event, the SEL-FLT will increment the Permanent Fault counter in the event statistics. The SEL-FLT then generates an exception Permanent Fault message (when enabled) to report the event. The SEL-FLT will start the Permanent Fault display local LED flash pattern. The SEL-FLT is unarmed at the end of the T_{FLT} timer after detecting a permanent fault event, and it will begin checking system conditions for a power restoration.

Momentary Fault

To register a momentary fault event, the SEL-FLT must first detect a fault stimulus followed by a protection operation. Then it must detect successful power restoration before the end of the configurable Fault Time-Out (T_{FLT}) period.

After detecting a fault stimulus, the SEL-FLT will start the T_{FLT} timer. The SEL-FLT will check for a protection operation, indicated by a loss of current. The SEL-FLT must also detect a successful power restoration as indicated by cur-

rent measured above the I_{ARM} threshold. If a loss of current is detected and load current is present at the end of the T_{FLT} period, the SEL-FLT will register a momentary fault event. *Figure 8.17* shows a sample load current (I_{LOAD}) profile (in rms) that results in the SEL-FLT registering a momentary fault event.

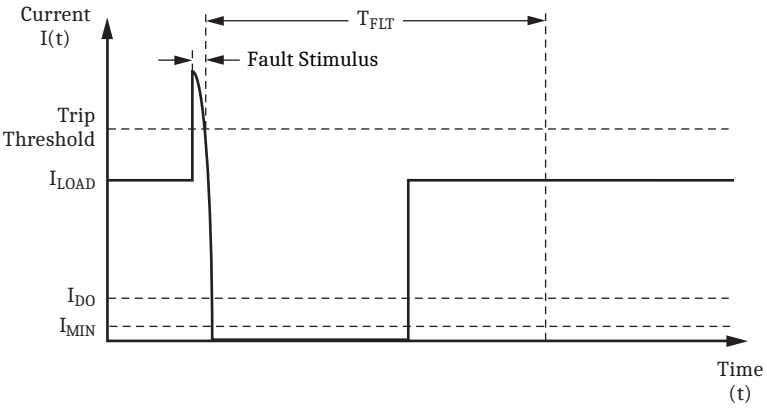


Figure 8.17 Momentary Fault

After detecting a momentary fault event, the SEL-FLT will increment the Momentary Fault counter in the event statistics. The SEL-FLT then generates an exception Momentary Fault message (when enabled) to report the event. The device also starts the local LED flash pattern when configured to display the event. After detecting a momentary fault event, the SEL-FLT will arm and set the active trip threshold based on load current measured at the end of the T_{FLT} timer.

Disturbance

To register a disturbance event, the SEL-FLT must detect a fault stimulus that is *not* followed by any protection operation during the Fault Time-Out (T_{FLT}) period.

After detecting a fault stimulus, the SEL-FLT will start the T_{FLT} timer. The SEL-FLT will check for a protection operation indicated by a loss of current. If a loss of current is not detected and load current is present at the end of the T_{FLT} timer, the SEL-FLT will register a disturbance event. *Figure 8.18* shows a sample load current (I_{LOAD}) profile (in rms) that results in the SEL-FLT registering a disturbance event.

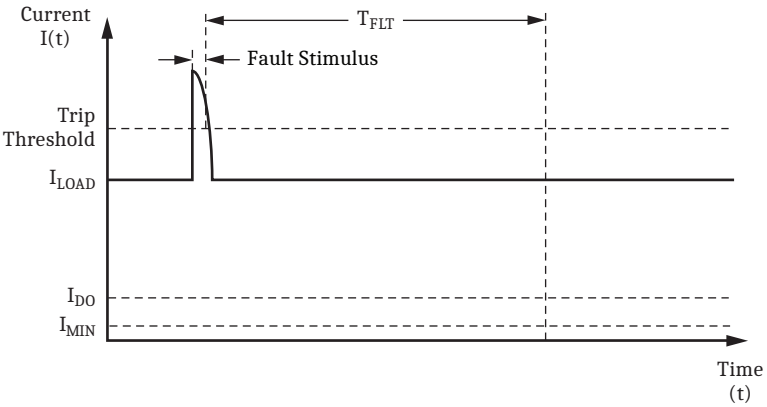


Figure 8.18 Disturbance

After detecting a Disturbance event, the SEL-FLT will increment the Disturbance counter in the event statistics. The SEL-FLT then generates an exception Disturbance message (when enabled) to report the event. The device also starts the local LED flash pattern when configured to display the event. After detecting a disturbance event, the SEL-FLT will arm and set the active trip threshold based on load current measured at the end of the T_{FLT} period.

Coordination Alarm

A Coordination alarm indicates a conflict between the SEL-FLT trip settings and the system conditions. The SEL-FLT registers a Coordination alarm when the sustained load current is measured in excess of the highest enabled trip threshold.

After detecting a fault stimulus, the SEL-FLT will start the T_{FLT} timer. If the load current is greater than the highest enabled AutoRANGE trip threshold at the end of the T_{FLT} period, a Coordination alarm is set. The device will not arm while a Coordination alarm is set. *Figure 8.19* shows a sample load current (I_{LOAD}) profile (in rms) that results in the SEL-FLT registering a Coordination alarm.

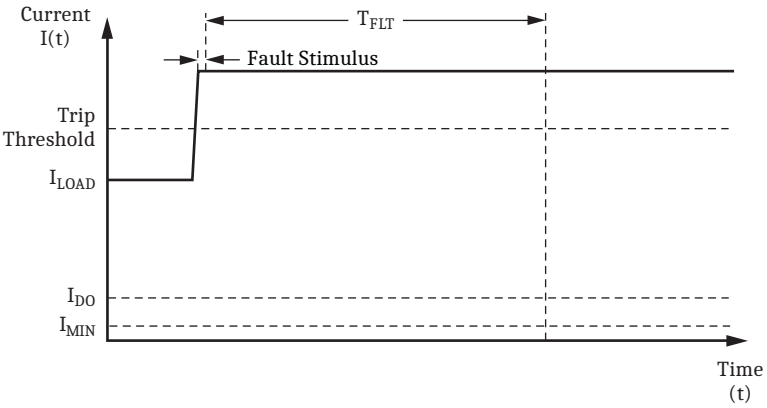


Figure 8.19 Coordination Alarm

After detecting a coordination alarm event, the SEL-FLT will increment the Coordination Alarm counter in the event statistics. The SEL-FLT then generates an exception Coordination Alarm message (when enabled) to report the event. The SEL-FLT is unarmed at the end of the T_{FLT} timer after detecting a coordination alarm event. Load current must be measured lower than the highest enabled AutoRANGE trip threshold for the System Arming Period (T_{ARM}) to clear the Coordination alarm.

Fault Magnitude

The SEL-FLT will measure the fault current magnitude as high as 1600 A during a Fault Stimulus event. The SEL-FLT will report the highest half-cycle fault current measured (in rms) in the fault event message. If the fault current exceeds 1600 A, the SEL-FLT reports the fault magnitude as 1600 A. The fault current magnitude is only measured during the fault stimulus event, and not after an outage detection (i.e., inrush fault currents as a result of reclosing are not measured).

SECTION 9

Maintenance, Testing, and Troubleshooting

Overview

This section provides guidelines for maintaining, testing, and troubleshooting the SEL-FLT and SEL-FLR system. Included are discussions on testing philosophies, methods, and tools. Troubleshooting may involve the SEL-FLT devices, the SEL-FLR, or both components of the system.

This section includes the following:

Maintenance

The SEL-FLT and SEL-FLR are designed to be maintenance-free, minimizing your total cost of ownership.

SEL-FLT Battery Safety

⚠WARNING

Batteries should always be handled with care and only by trained personnel. Failure to comply with safety procedures of the battery manufacturer could result in serious injury.

In the event of a puncture, rupture, or other damage to the lithium metal cell, do not return the product to SEL. Immediately dispose of the product in accordance with local disposal guidelines for lithium metal cells.

Cleaning the SEL-FLR

Use care when cleaning the SEL-FLR. Use a mild soap or detergent solution and a damp cloth to clean the chassis. Do not use abrasive materials, polish compounds, or harsh chemical solvents (such as xylene or acetone) on any surface.

Testing

The SEL-FLT event detection feature can be tested through the use of a current loop before installation. This allows for optional commissioning of the SEL-FLT prior to deployment.

Equipment

CRSRTT Magnet Tool

The CRSRTT magnet tool (SEL part number CRSRTT; see *Figure 9.1*) is used to interact with the SEL-FLT. Use the magnet tool to activate the radio in the SEL-FLT and to reset the unit after each test. Remove the protective shorting bar (shown in *Figure 9.1*) before using the magnet tool. Replace the shorting bar after use.

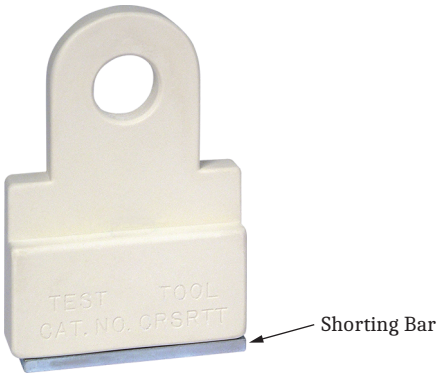


Figure 9.1 CRSRTT Magnet Tool

MCL120 Mini Current Loop

⚠CAUTION
Do not press the pushbutton on the MCL120 for longer than 10 seconds per minute.

The following test steps use a Mini Current Loop (see *Figure 9.2*) to simulate load and fault conditions. When energized, a magnetic field equivalent to approximately 10 A continuously circulates through the loop. When the integral pushbutton plunger is depressed, an equivalent magnetic field of approximately 1000 A is produced, which will trip the SEL-FLT. The Mini Current Loop is sold separately (SEL part number MCL120).

Figure 9.2 Mini Current Loop

Although the test below specifically uses a Mini Current Loop for testing, any current loop capable of injecting fault currents can be used.

Install the SEL-FLT on the Mini Current Loop.

Permanent Fault Test

This test will execute a permanent fault event. *Figure 9.3* shows the current profile as a result of executing the steps in *Table 9.1*.

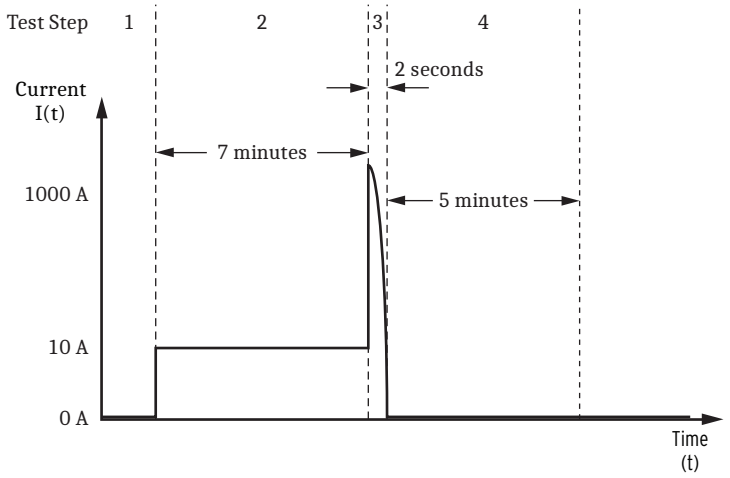


Figure 9.3 Permanent Fault Test

Table 9.1 Permanent Fault Test

Step	Test Parameters			Test Results	
	MCL	Current (A)	Duration	Display	Message
1	Unplugged	0	—	Off	—
2	Plugged In	10	7 minutes	Arm (after 5 minutes)	Restoration (after 5 minutes)
3	Pushed	1000	2 seconds	Permanent Fault	Fault Stimulus (if enabled)
4	Unplugged	0	5 minutes	Permanent Fault	Permanent Fault (after 5 minutes)

Step 1. Install the SEL-FLT on a de-energized (unplugged) current loop with 0 A of current.

Step 2. Provide 10 A of load current for 7 minutes by plugging the MCL120 into a power outlet.

The SEL-FLT sends a Restoration message and flashes the Arm display 5 minutes after current is applied.

Step 3. Inject a 1000 A fault current for 2 seconds by pressing the plunger on MCL120.

The SEL-FLT will send a Fault Stimulus message (if enabled) and start the Permanent Fault flash display.

Step 4. Remove current from the SEL-FLT by unplugging the MCL120.

The SEL-FLT sends a Permanent Fault message 5 minutes after the fault current is applied.

Momentary Fault Test

This test will execute a momentary fault event. *Figure 9.4* shows the current profile as a result of executing the steps in *Table 9.2*.

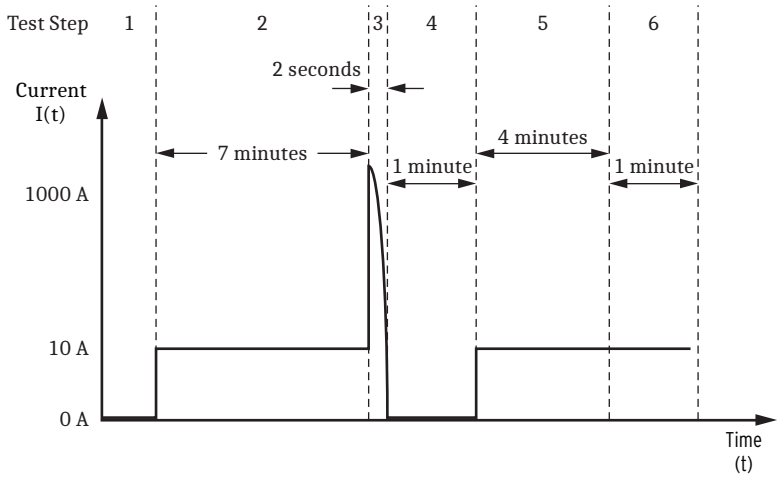


Figure 9.4 Momentary Fault Test

Table 9.2 Momentary Fault Test

Step	Test Parameters			Test Result	
	MCL	Current (A)	Duration	Display	Message
1	Unplugged	0	—	Off	—
2	Plugged In	10	7 minutes	Arm (after 5 minutes)	Restoration (after 5 minutes)
3	Pushed	1000	2 seconds	Permanent Fault	Fault Stimulus (if enabled)
4	Unplugged	0	1 minute	Permanent Fault	—
5	Plugged In	10	4 minutes	Permanent Fault	—
6	Plugged In	10	1 minute	Local Display (if enabled)	Momentary Fault (if enabled)

Step 1. Install the SEL-FLT on a de-energized (unplugged) current loop with 0 A of current.

Step 2. Provide 10 A of load current for 7 minutes by plugging the MCL120 into a power outlet.

The SEL-FLT sends a Restoration message and flashes the Arm display 5 minutes after current is applied.

Step 3. Inject a 1000 A fault current for 2 seconds by pressing the plunger on MCL120.

The SEL-FLT sends a Fault Stimulus message (if enabled) and starts the Permanent Fault flash display.

Step 4. Remove current from the SEL-FLT for 1 minute by unplugging the MCL120.

Step 5. Provide 10 A of load current for 5 minutes by plugging the MCL120 into a power outlet.

Step 6. The SEL-FLT sends a Momentary Fault message and starts the Local display flash pattern (if enabled).

Permanent Loss-of-Current Test

This test will execute a permanent loss-of-current event. *Figure 9.5* shows the current profile as a result of executing the steps in *Table 9.3*.

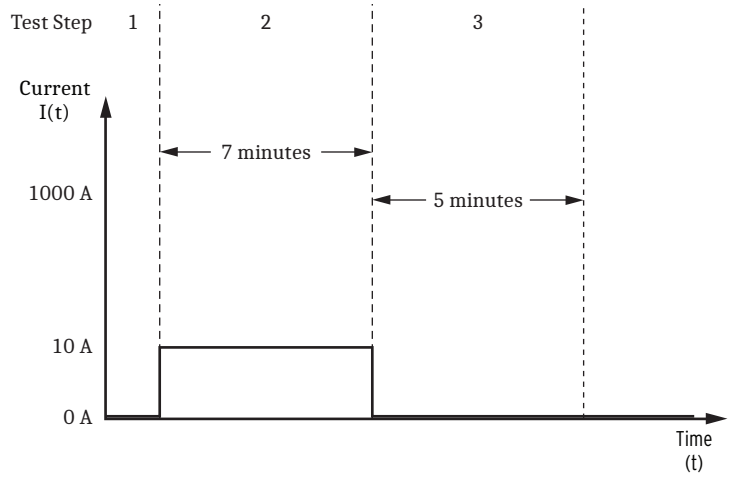


Figure 9.5 Permanent Loss-of-Current Test

Table 9.3 Permanent Loss-of-Current Test

Step	Test Parameters			Test Results	
	MCL	Current (A)	Duration	Display	Message
1	Unplugged	0	—	Off	—
2	Plugged In	10	7 minutes	Arm (after 5 minutes)	Restoration (after 5 minutes)
3	Unplugged	0	5 minutes	Local Display (if enabled)	Permanent LOC (after 5 minutes) (if enabled)

Step 1. Install the SEL-FLT on a de-energized (unplugged) current loop with 0 A of current.

Step 2. Provide 10 A of load current for 7 minutes by plugging the MCL120 into a power outlet.

The SEL-FLT will send a Restoration message and flash the Arm display 5 minutes after current is applied.

Step 3. Remove current from the SEL-FLT by unplugging the MCL120.

The SEL-FLT sends a Permanent LOC message (if enabled) 5 minutes after current is removed. The SEL-FLT also starts the Local LED display if the Enable Permanent Loss-of-Current Display parameter is enabled.

Momentary Loss-of-Current Test

This test will execute a momentary loss-of-current event. *Figure 9.6* shows the current profile as a result of executing the steps in *Table 9.4*.

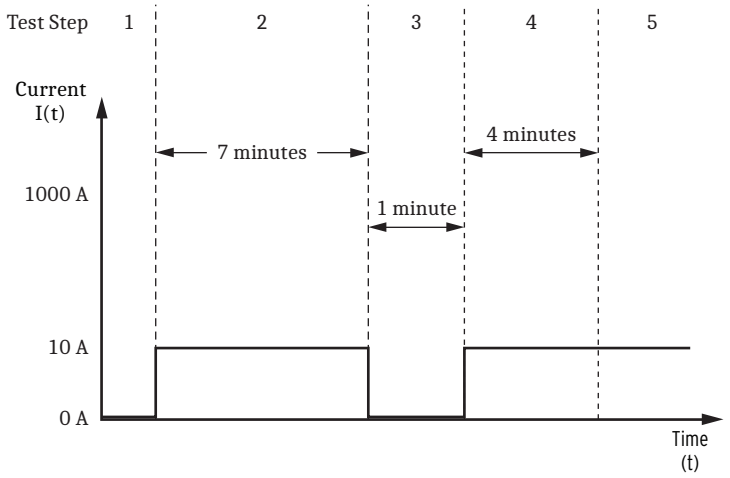


Figure 9.6 Momentary Loss-of-Current Test

Table 9.4 Momentary Loss-of-Current Test

Step	Test Parameters			Test Results	
	MCL	Current (A)	Duration	Display	Message
1	Unplugged	0	—	Off	—
2	Plugged In	10	7 minutes	Arm (after 5 minutes)	Restoration (after 5 minutes)
3	Unplugged	0	1 minute	Off	—
4	Plugged In	10	4 minutes	Off	—
5	Plugged In	10	1 minute	Off	Momentary LOC (if enabled)

Step 1. Install the SEL-FLT on a de-energized (unplugged) current loop with 0 A of current.

Step 2. Provide 10 A of load current for 7 minutes by plugging the MCL120 into a power outlet.

The SEL-FLT sends a Restoration message and flashes the Arm display 5 minutes after current is applied.

Step 3. Remove current from the SEL-FLT for 1 minute by unplugging the MCL120.

Step 4. Provide 10 A of load current for 5 minutes by plugging the MCL120 into a power outlet.

Step 5. The SEL-FLT sends a Momentary LOC message (if enabled) 5 minutes after current is removed.

Troubleshooting

SEL-FLR Inspection Procedure

If you suspect a problem with your SEL-FLR, complete the following procedure before making any adjustments to the device. After you finish your inspection, refer to *Table 9.5*.

Step 1. Record a description of any problem you encountered.

Step 2. Record the states of the LED indicators.

Step 3. Record recent and present environmental conditions and any system events.

Step 4. If the web interface is accessible, record the part number, serial number, and firmware version from the **SEL-FLR Dashboard**. In addition, examine the **Local Syslog Events** and **Major Alarm** pages and record any unusual values.

Step 5. Export the device Syslog report and device settings.

Troubleshooting Procedure

Table 9.5 lists troubleshooting procedures for common problems. This table lists symptoms, possible causes, and corresponding diagnoses and solutions.

Table 9.5 Troubleshooting Procedure (Sheet 1 of 5)

Issue/Indicator	Possible Causes	Test and Solution
Device will not start, is nonresponsive, or the **ENABLED** and **ALARM** LEDs are not illuminated.	Input power is not present or power supply connector is not fully seated.	Remove power source. Verify power cabling and ground connections. Remove power supply connector(s) and reseat. Reconnect power source.
	Power supply is out of tolerance.	Measure and record the power supply voltage at the power input terminals. Verify that the measured value falls within the rated range listed in *SEL-FLR Specifications* on page 1.11.
The **ENABLED** LED is not illuminated and the **ALARM** LED is illuminated.	Device has experienced a diagnostics failure that prevents it from operating.	Perform the steps in *SEL-FLR Inspection Procedure* on page 9.7. Contact Schweitzer Engineering Laboratories, Inc. for further support.
The **ETH F**, **ETH 1**, or **ETH 2** yellow LED is flashing.	A network communication collision is detected.	Configure attached network devices for full-duplex communications.
The **ETH F**, **ETH 1**, or **ETH 2** yellow LED is off after making a connection, or network speeds are slower than expected.	Attached network device is configured for 10 Mbps.	Set connection settings for the attached network device to 100 Mbps or Auto Sense.

Table 9.5 Troubleshooting Procedure (Sheet 2 of 5)

Issue/Indicator	Possible Causes	Test and Solution
The **ETH F**, **ETH 1**, or **ETH 2** green LED is off after making a connection.	The attached network device interface is disabled.	Enable the attached network device interface.
	The Ethernet cabling is faulty.	Inspect cabling and replace if necessary.
	The interface is disabled (**ETH 1** and **ETH 2** only).	Enable the interface on the SEL-FLR. See *Ethernet Network Interfaces* on page 4.15.
The SEL-FLR will not reliably join with either a particular SEL-FLT or to a subset of installed SEL-FLT devices (but other SEL-FLT devices are successfully communicating with the SEL-FLR).	The SEL-FLT has not been activated.	The SEL-FLT ships from the factory in a deep-sleep mode and must be manually activated before installation. For more information, see *Section 2: Installation*.
	The SEL-FLT has been replaced without updating the SEL-FLT whitelist with the new Device Address.	Ensure the SEL-FLT Device Address appears in the whitelist display. See *SEL-FLT Sensor Management* on page 4.12.
	There is an obstructed radio path between the SEL-FLR and affected SEL-FLT devices caused by terrain, vegetation, snow cover, or intervening structures.	Navigate to the **SEL-FLT Dashboard** page on the SEL-FLR web interface. Compare the signal quality readings of installed SEL-FLT devices to identify poorly performing links. Check for obstructions and perform a path study if necessary. Consider relocating the affected SEL-FLT devices to a more advantageous location or relocating or raising the SEL-FLR antenna. Consider changing the SEL-FLR antenna type. See *SEL-FLR Configuration* on page 4.1 and *Appendix D: Link Budget Analysis* for more information.
	The network may be in the process of reacquiring SEL-FLT devices and exchanging encryption keys after an SEL-FLR power loss, a change in wireless frequency (radio channel), a device reset, a settings change, or a firmware upgrade.	Verify the SEL-FLT is on the whitelist. Wait for 75 minutes. If the SEL-FLT is still not reporting, there may be a path obstruction or a problem with the SEL-FLT itself.
	The SEL-FLT is already joined to another SEL-FLR. (We will refer to this as the remote SEL-FLR.)	There is no local method to regain pairing with an SEL-FLT that is actively joined to another network. To break a communications link, remove the SEL-FLT from the whitelist on the remote SEL-FLR. After several minutes, the SEL-FLT will appear in the Discovery list of the local SEL-FLR as an unjoined device. Move the SEL-FLT to the whitelist to start the joining process.
	A strong interfering radio source is affecting signal reception by the SEL-FLT devices in a particular location, rendering them unable to receive the signals required for network operation from the SEL-FLR.	Use the site analysis tool to determine whether there are interfering signals on the present network channel. Switch the network to a channel with less interference.
	The SEL-FLR antenna is improperly mounted, a cable is damaged, or a connector is soiled or loose.	Ensure that the antenna is properly installed and that the cable connections have proper seals. Inspect the cable for damage. **Note:** Nearby SEL-FLT devices with a good radio path may have sufficient signal strength to work even through a compromised antenna system.

Table 9.5 Troubleshooting Procedure (Sheet 3 of 5)

Issue/Indicator	Possible Causes	Test and Solution
	The SEL-FLT radio is in back-off mode.	Verify the SEL-FLT is on the whitelist. Wait 15 minutes. If the SEL-FLT is still not reporting, there may be a path obstruction or a problem with the SEL-FLT itself.
	The SEL-FLT has failed.	Contact SEL.
	The SEL-FLT and SEL-FLR firmware versions are not compatible.	Contact SEL.
The **LINK QUALITY** LEDs on the SEL-FLR front panel only have the red or yellow LEDs illuminated.	The wireless link quality for one or more SEL-FLT is less than ideal.	One or more SEL-FLT devices have poor link quality. Navigate to the **SEL-FLT Dashboard** page on the web interface and examine the RSSI value of each SEL-FLT. The RSSI should ideally be between –50 and –80 dB. If the value falls outside of this range, the link quality may be less than ideal. See *Appendix D: Link Budget Analysis* for more information. If the problem persists, consider relocating the SEL-FLT to a more favorable area or relocating or raising the SEL-FLR antenna.
Communications link failures with all SEL-FLT devices.	SEL-FLR antenna or cable is disconnected or damaged.	Ensure that the antenna is properly installed and the cable connections have proper seals. Inspect the cable for damage.
	There is an obstructed radio path between the SEL-FLR and affected SEL-FLT devices caused by terrain, vegetation, snow cover, or intervening structures.	Navigate to the **SEL-FLT Dashboard** on the SEL-FLR web interface. Compare the signal quality readings of installed SEL-FLT devices to identify poorly performing links. Check for obstructions and perform a path study if necessary. Consider relocating the affected SEL-FLT devices to a more advantageous location or relocating or raising the SEL-FLR antenna. Consider changing the SEL-FLR antenna type. See *Section 4: SEL-FLR Configuration* and *Appendix D: Link Budget Analysis* for more information.
	Improper cable is being used, or cable length is too long.	Verify that correct cables are used and that cable connections and length are valid. See *Appendix D: Link Budget Analysis*.
	Interfering signals are inhibiting SEL-FLR and SEL-FLT wireless communication.	Inspect the SEL-FLR location. Use the site analysis tool to determine whether there are interfering signals on the present network channel. Select a different network frequency (radio channel) to avoid the interference. See *SEL-FLR Radio Network Settings* on page 4.6 for more information.
The login page is inaccessible from the front-panel **ETH F** interface.	The **ETH F** network interface is not enabled.	Reset the **ETH F** port (see *Device Reset* on page 5.18 for instructions).
	DHCP is disabled on **ETH F** and the management computer is not configured with a static IP address.	Verify the physical and logical connection between the management computer and the SEL-FLR. Configure the IP address for the network adapter of the management computer to the same network as the SEL-FLR. See *Appendix F: Configuring Windows Network Parameters* for more information.

Table 9.5 Troubleshooting Procedure (Sheet 4 of 5)

Issue/Indicator	Possible Causes	Test and Solution
	DHCP is enabled on **ETH F** and the management computer is configured with a static IP address.	Verify the physical and logical connection between the management computer and the SEL-FLR. Configure the network adapter for the management computer to obtain an IP address automatically. See *Appendix F: Configuring Windows Network Parameters* for more information.
	DHCP is enabled on **ETH F** and the management computer is using Google Chrome version 63 or later.	Reset the **ETH F** port through the pinhole reset. See *Pinhole Reset* on page 5.19 for more information. Configure the IP address for the network adapter of the management computer to the same network as the SEL-FLR. See *Appendix F: Configuring Windows Network Parameters* for more information.
A user cannot log in to the SEL-FLR web interface.	The user's account is missing or disabled.	Log in to the SEL-FLR as an Administrator or User Manager and verify the details of the user's account. See *User Accounts* on page 5.5 for more information.
	The user's password is incorrect.	Log in to the SEL-FLR as an Administrator or User Manager and reset the password for the user's account. See *User Accounts* on page 5.5 for more information.
No remote Syslog messages are received from the SEL-FLR.	No Syslog servers are defined.	Set up a remote Syslog destination. See *Syslog Reporting* on page 6.4 for more information.
	The Syslog severity threshold is unexpectedly high.	Reconfigure the severity threshold for the remote Syslog destination to the desired severity level. See *Syslog Reporting* on page 6.4 for more information.
	The Syslog server is not reachable from the network containing the SEL-FLR.	Ensure that the Syslog server IP address is valid and reachable. See *Syslog Reporting* on page 6.4 for more information.
	The SEL-FLR network gateway is not configured.	If the Syslog server is on another network, ensure that a network gateway is configured and available to route the Syslog traffic.
Not receiving all expected remote Syslog messages.	The remote Syslog severity threshold is unexpectedly high.	Reconfigure the severity threshold for the remote Syslog destination to the desired security level. See *Syslog Reporting* on page 6.4 for more information.
Date and time are incorrect (and no DNP3 time source is connected).	The SEL-FLR clock battery is depleted.	Replace only with Rayovac no. BR1632 or equivalent recommended by manufacturer.
Time (hour) is incorrect in the local Syslog report.	The UTC offset parameter is incorrectly entered.	Set the Local Time Zone Offset from UTC. See *Date/Time Settings* on page 5.1 for more information.
The SEL-FLT misses a fault.	The trip threshold is set too high.	Lower the trip threshold setting (see *AutoRANGE Trip Threshold* on page 4.31).
	The delay trip is set too long.	Decrease the delay trip setting (see *AutoRANGE Trip Threshold* on page 4.31).

Table 9.5 Troubleshooting Procedure (Sheet 5 of 5)

Issue/Indicator	Possible Causes	Test and Solution
The SEL-FLT does not arm.	The arming settings are too high.	Change the I_{ARM} setting to below load current levels (see *Current Arming Threshold (I_{ARM})* on page 4.29).
	There is insufficient load present.	Review the SEL-FLT arming requirements (see *Device Arming* on page 8.1). Select a deployment location with sufficient load.

Warranty and Returns

The SEL-FLT and SEL-FLR are covered by the standard SEL ten-year warranty. For warranty details, visit selinc.com or contact your customer service representative. Should the SEL-FLT need to be returned or shipped for any reason, follow local regulations for shipping the product.

Transportation Regulations

NOTE: The SEL-FLT contains 5.06 grams of $LiSOCl_2$.

The SEL-FLT product is shipped with or contains a lithium metal cell. Lithium metal cells are often classified as dangerous goods by dangerous goods shipment regulations. These regulations, along with your package carrier, specify the packaging and labeling to be used, along with the information to be provided when shipping dangerous goods. This product must be transported in accordance with all applicable rules, laws, and regulations, such as the rules published by the Pipeline and Hazardous Materials Safety Administration; the International Civil Aviation Organization; the International Air Transport Association; the Maritime Dangerous Goods Code; the UN Model Regulations on the Transport of dangerous Goods; and rules for inland, waterways, road, and rail transportation, and others. Please consult any applicable regulations and your package carrier for proper handling of this product.

Technical Support

Obtain technical assistance from the following:

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

This page intentionally left blank

APPENDIX A

Firmware and Manual Versions

Firmware

Determining the Firmware Version

To determine the SEL-FLR firmware version, navigate to the **Dashboard > SEL-FLR Dashboard** page. The firmware version is shown under the device information heading, as shown in *Figure A.1*.

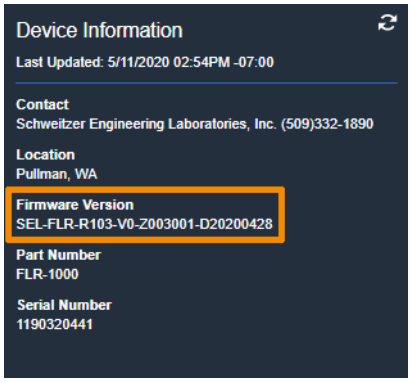


Figure A.1 SEL-FLR Firmware Version Identification

The firmware version number is after the R, and the date code is after the D. For example, the following is SEL-FLR firmware version number R100, date code December 03, 2014.

FID=SEL-FLR-R100-V0-Z001001-D20141203

To determine the SEL-FLT firmware version, navigate to the **Dashboard > SEL-FLT Dashboard** page. Click an SEL-FLT device to show all of the device details. In the search bar, type **firmware** to find the SEL-FLT firmware version, as shown in *Figure A.2*.

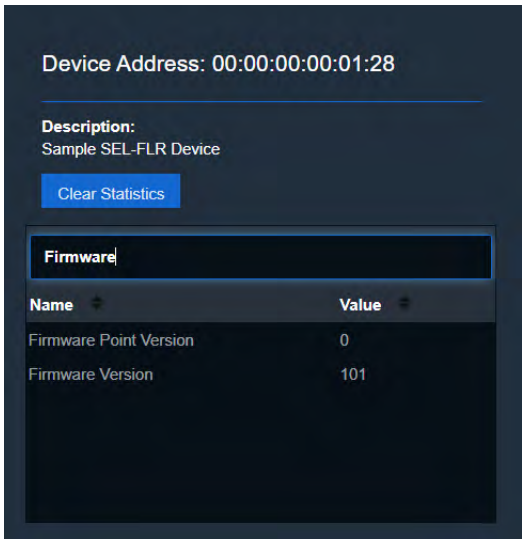


Figure A.2 SEL-FLT Firmware Version Identification

Revision History

Table A.1 and *Table A.2* list the firmware versions, revision descriptions, and corresponding instruction manual date codes. The most recent firmware version is listed first.

Starting with revisions published after March 1, 2022, changes that address security vulnerabilities are marked with "[Cybersecurity]". Improvements to cybersecurity functionality that should be evaluated for potential cybersecurity importance are marked with "[Cybersecurity Enhancement]".

Table A.1 SEL-FLR Firmware Revision History (Sheet 1 of 3)

Firmware Identification (FID) Number[a]	Summary of Revisions	Manual Date Code
SEL-FLR-R104-V0-Z003001-D20220401	➤ Added channel mapping to support Argentina (FLR-1008). ➤ Addressed an issue that caused the logging of a firmware upgrade to fail if the upgrade required a settings conversion. Therefore, any firmware upgrade from previous versions to this version will erase the syslog. ➤ Changed the maximum network size to 96 SEL-FLT devices. ➤ Added support for multiple DNP sessions. ➤ Added support for a single anonymous DNP session.	20220401
SEL-FLR-R103-V3-Z003001-D20210303	Includes all the functions of SEL-FLR-R103-V2-Z003001-D20200916 with the following additions: ➤ Addressed an issue that, in all previous versions, could cause the SEL-FLR to no longer communicate through the DNP3 or web interface. In previous versions, actions by an unauthorized user could cause the SEL-FLR to become unresponsive in rare cases. In this situation, a manual restart was required to restore functionality. ➤ Addressed CVE-2019-11477, where in all previous versions, maliciously crafted Ethernet packets could cause a denial of service. ➤ Addressed an issue that, in all previous versions, could cause the SEL-FLR DNP3 server to fail to return to online status after DNP3 settings changes.	20210415

Table A.1 SEL-FLR Firmware Revision History (Sheet 2 of 3)

Firmware Identification (FID) Number[a]	Summary of Revisions	Manual Date Code
	➤ Addressed an issue with high levels of Ethernet traffic that, in all previous versions, could cause the SEL-FLR rear-panel Ethernet interface to stop transmitting. In this situation, the user needed to reboot the SEL-FLR or disable and re-enable the rear-panel Ethernet interface. This behavior could be triggered by a high volume of traffic being sent and received. ➤ Addressed an issue that, in all previous versions, prevented the SEL-FLR pinhole reset procedure from resetting the front-panel Ethernet interface if the default address was already assigned to the front port.	
SEL-FLR-R103-V2-Z003001-D20200916	Includes all the functions of SEL-FLR-R103-V1-Z003001-D20200904 with the following addition: ➤ Added channel mapping to support Ecuador (FLR-1009).	20200925
SEL-FLR-R103-V1-Z003001-D20200904	Includes all the functions of SEL-FLR-R103-V0-Z003001-D20200428 with the following additions: ➤ Addressed issue that, in previous firmware versions, caused the DNP3 server to unexpectedly fail during operation or as the result of a device restart when 14 or more SEL-FLT devices are mapped in the DNP3 block. ➤ Addressed issue that, in all previous firmware versions, may prevent whitelisted SEL-FLT devices from rejoining the network after the radio network was automatically restarted. ➤ Addressed issue that, in all previous firmware versions, caused high SEL-FLR RAM utilization after removing SEL-FLT devices from the whitelist after frequent network unjoin/join activity, or when many SEL-FLT devices were mapped in DNP. These high RAM usage situations slowed the user interface responsiveness, and in some cases caused the DNP3 server to stop responding, requiring a restart. ➤ Addressed issue that, in firmware version R103-V0, could cause the rear-panel Ethernet ports to become disabled after a port settings change. In this situation, a manual restart was required to restore port functionality.	20200904
SEL-FLR-R103-V0-Z003001-D20200428	➤ Improved error handling and display messages on the user interface. ➤ Addressed issue that, in all previous firmware versions, caused the SEL-FLR to improperly display Long Update Interval load data while the SEL-FLT was experiencing low-load conditions. ➤ Added RSSI and Packet Error Rate DNP3 analog input data points to the data map for each SEL-FLT. ➤ Improved the radio protocol to decrease susceptibility to interference from other wireless networks. ➤ Addressed issue that, in all previous firmware versions, caused the rear Ethernet ports to have significant delays in servicing Ethernet traffic. ➤ Removed the SEL-FLT setting Enable Momentary Loss-of-Current Display from the web interface. ➤ Added support for incoming ping (echo requests) on the SEL-FLR Ethernet interfaces. ➤ Modified firmware to ensure the radio spectrum complies with FCC requirements for power spectral density. In previous firmware versions, the radio spectrum exceeded FCC requirements for power spectral density. ➤ Added support for channel mapping in international regions. In previous firmware versions, channel mapping was exclusive to North America.	20200529

Table A.1 SEL-FLR Firmware Revision History (Sheet 3 of 3)

Firmware Identification (FID) Number[a]	Summary of Revisions	Manual Date Code
SEL-FLR-R102-V0-Z001001-D20190701	➤ Enhanced the over-the-air firmware upgrade capabilities for the SEL-FLT to continue the upgrade when the node rejoins the network. ➤ Addressed issue that, in all previous firmware versions, may prevent whitelisted SEL-FLT devices from rejoining the network when the radio network was previously disabled. ➤ Addressed issue that, in all previous firmware versions, may cause the SEL-FLR to restart when the radio becomes unresponsive. ➤ Modified the firmware to change the default setting for Captive Port on the ETH F port to disabled. In previous firmware, the Captive Port was enabled by default for the ETH F port. ➤ Addressed issue where, in all previous firmware versions, the scroll bar behavior was not supported on Google Chrome version 76 or later. ➤ Addressed issue where, in all previous firmware versions, the spectrum scan average RSSI results were not being properly computed.	20190816
SEL-FLR-R101-V1-Z001001-D20190212	Includes all the functions of SEL-FLR-R101-V0-Z001001-D20181220 with the following addition: ➤ Addressed an issue in firmware version R101 that caused the SEL-FLR to send incorrect settings over-the-air to SEL-FLT devices.	20190212
SEL-FLR-R101-V0-Z001001-D20181220	➤ Initial version.	20181220

[a] SEL-FLR firmware versions R103-V0 and later are not compatible with SEL-FLT firmware versions R100-V1 and earlier.

Table A.2 SEL-FLT Firmware Revision History (Sheet 1 of 2)

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-FLT-R101-V0-Z001001-20200427 **Note:** SEL-FLT firmware version R101-V0 is not compatible with SEL-FLR firmware version R102-V0 and earlier.	➤ Addressed issue that, in all previous firmware versions, may prevent joined SEL-FLT devices from unjoining from the SEL-FLR network or transmitting data. ➤ Improved the radio protocol to decrease susceptibility to interference from other wireless networks. ➤ Improved handling of calibration memory errors. ➤ Improved the SEL-FLT to allow over-the-air firmware upgrades that have new protocol versions. ➤ Modified firmware to ensure the radio spectrum complies with FCC requirements for power spectral density. In previous firmware versions, the radio spectrum exceeded FCC requirements for power spectral density.	20200529
SEL-FLT-R100-V1-Z001001-D20190816 **Note:** Prior to upgrading SEL-FLT devices to firmware version R100-V1, upgrade the SEL-FLR to firmware version R102 or later.	Includes all the functions of SEL-FLT-R100-V0-Z001001-D20181116 with the following additions: ➤ Added support for memory logging after a device error. ➤ Addressed issue that, in all previous firmware versions, would cause the SEL-FLT device to unjoin from the network at extreme hot and cold ambient temperatures. ➤ Addressed issue that, in all previous firmware versions, may cause the SEL-FLT device to communicate at a lower than specified transmit power. ➤ Addressed issue that, in all previous firmware versions, may increase the time required for an SEL-FLT device to join a network. ➤ Addressed issue that, in all previous firmware versions, may cause the SEL-FLT to unjoin from the network because of an unmanaged radio reset.	20190816

Table A.2 SEL-FLT Firmware Revision History (Sheet 2 of 2)

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
	➤ Addressed issue that, in all previous firmware versions, may cause the SEL-FLT device to reset because of a number of messages being queued up for transmission. ➤ Addressed issue where, in all previous firmware versions, when the SEL-FLT radio is turned on, the device may continuously reset. ➤ Addressed issue where, in all previous firmware versions, the SEL-FLT radio may not rejoin the network after becoming unjoined.	
SEL-FLT-R100-V0-Z001001-D20181116 **Note:** When upgrading SEL-FLT devices with firmware version R100, disable the Short Update Interval parameter prior to upgrading units.	➤ Initial version.	20181220

Instruction Manual

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

Table A.3 lists the instruction manual versions and revision descriptions. The most recent instruction manual version is listed first.

Table A.3 Instruction Manual Revision History (Sheet 1 of 4)

Date Code	Summary of Revisions
20230106	Section 1 ➤ Updated *Specifications*.
20220401	General ➤ Added Argentina certification details for FLT-1008 and FLR-1008 models. Section 4 ➤ Added note to *Firmware Upgrade Performance* and *Adding SEL-FLT Devices*. ➤ Updated *Table 4.4: Whitelist Attribute Fields*. ➤ Added *Multisession*. ➤ Updated *Settings* and *DNP Communication*. ➤ Added note to *Time Synchronization*. ➤ Updated *Table 4.13: Ethernet Port DNP3 Protocol Settings*. ➤ Updated *Figure 4.21: DNP3 Address Setup*. ➤ Updated *Component Removal and Block Remap*. Section 5 ➤ Updated *Time Source*. ➤ Added note to *Import Settings*. Section 9 ➤ Updated *Table 9.5: Troubleshooting Procedure*. Appendix A ➤ Updated for firmware version R104.
20220304	Section 1 ➤ Updated *System Features and Benefits* and *Specifications*.

Table A.3 Instruction Manual Revision History (Sheet 2 of 4)

Date Code	Summary of Revisions
20210701	**General** ➤ Added information for optional SEL-FLR enclosure. ➤ Added *Appendix H: SEL-FLR Enclosure*. ➤ Updated range between SEL-FLR and connected SEL-FLT devices to 400 m (0.25 mi). **Section 2** ➤ Added *Field Connections to the Enclosure*, *Installing the Enclosure*, and *Enclosure Maintenance*.
20210415	**General** ➤ Added channel information and certification details for FLT-1003 and FLR-1003 models (Peru). ➤ Removed references to Momentary Loss-of-Current local event display feature, which was removed in SEL-FLR firmware version R103-V0. ➤ Removed FLT-1000 and FLR-1000 Colombia references. **Section 1** ➤ Updated *Table 1.1: SEL-FLT and SEL-FLR Models by Country*. ➤ Updated *Table 1.5: SEL-FLR Certifications by Country*. **Section 4** ➤ Updated *Table 4.1: SEL-FLR Radio Settings*. ➤ Updated *Table 4.2: SEL-FLR Channel Mapping by Model/Country*. **Appendix A** ➤ Updated for firmware version R103-V3 for the SEL-FLR. ➤ Updated entry for firmware version R103-V1 for the SEL-FLR.
20201203	**General** ➤ Added Mexico certification details for FLT-1000 and FLR-1000 models. **Section 1** ➤ Updated *Table 1.1: SEL-FLT and SEL-FLR Models by Country*. ➤ Updated *SEL-FLT Specifications* and *SEL-FLR Specifications*. **Section 4** ➤ Updated *Table 4.2: SEL-FLR Channel Mapping by Model/Country*.
20201022	**General** ➤ Added channel information and certification details for FLT-1007 and FLR-1007 models (Costa Rica). **Section 1** ➤ Updated *Table 1.1: SEL-FLT and SEL-FLR Models by Country*. ➤ Updated *SEL-FLT Specifications* and *SEL-FLR Specifications*. **Section 4** ➤ Updated *Table 4.1: SEL-FLR Radio Settings* and *Table 4.2: SEL-FLR Channel Mapping by Model/Country*. ➤ Updated *Site Analysis*. **Appendix D** ➤ Updated *Transmitted and Radiated Power Requirements*.
20201006	**Section 1** ➤ Updated *Table 1.3: SEL-FLR Orderable Accessories*.
20200925	**General** ➤ Added channel information and certification details for FLT-1006 and FLR-1006 models (Brazil). ➤ Added channel information and certification details for FLT-1009 and FLR-1009 models (Ecuador). **Preface** ➤ Updated *Other Safety Marks*. ➤ Added *Wireless Regulatory Statements*.

Table A.3 Instruction Manual Revision History (Sheet 3 of 4)

Date Code	Summary of Revisions
	Section 1 ➤ Added *Table 1.1: SEL-FLT and SEL-FLR Models by Country*. ➤ Added footnote to *Table 1.2: SEL-FLR Orderable Accessories*. ➤ Updated *SEL-FLT Specifications* and *SEL-FLR Specifications* to include channel mapping differences by country and added *Certifications by Country* tables. **Section 2** ➤ Updated *Channel Selection*. **Section 4** ➤ Updated *Channel Selection*. ➤ Updated *Table 4.1: SEL-FLR Radio Settings* and *Table 4.2: SEL-FLR Channel Mapping by Model/Country*. **Section 5** ➤ Updated *File Management*. **Appendix A** ➤ Updated for firmware version R103-V2 for the SEL-FLR. **Appendix D** ➤ Updated *Transmitted and Radiated Power Requirements*. ➤ Added footnote to *Table D.2: Antenna Gain*.
20200904	**Section 4** ➤ Updated *DNP3 Data Sets* description. ➤ Updated *Component Removal and Block Remap* to explain how reserved space is managed. **Section 7** ➤ Updated description of long press. **Appendix A** ➤ Updated for firmware version R103-V1 for the SEL-FLR.
20200529	**General** ➤ Renamed *Section 5* from *Systems* to *System*. **Section 2** ➤ Updated *Enabling the SEL-FLR Network Radio* in *Getting Started*. **Section 4** ➤ Added *Ping* to *Ethernet Network Interfaces*. ➤ Updated *Table 4.6: ETH F Network Interface Settings* and *Table 4.7: ETH 1 and ETH 2 Network Interface Settings*. ➤ Updated *SEL-FLT Settings* in *SEL-FLT Parameters and Settings*. **Section 6** ➤ Updated *Figure 6.3: Alarm Notifications*. **Section 8** ➤ Updated *Figure 8.4: Outage Detection—Slow Dropout*. **Section 9** ➤ Updated *Table 9.5: Troubleshooting Procedure*. **Appendix A** ➤ Updated for firmware version R103-V0 for the SEL-FLR. ➤ Updated for firmware version R101-V0 for the SEL-FLT.
20190816	**Section 1** ➤ Updated *SEL-FLR Web Interface*. **Section 2** ➤ Updated *Physical Network*.

Table A.3 Instruction Manual Revision History (Sheet 4 of 4)

Date Code	Summary of Revisions
	Section 4 ➤ Updated *ETH F Interface Reset* and *Captive Port*. ➤ Updated *Table 4.6: ETH F Network Interface Settings*. **Section 5** ➤ Updated *Export Settings*. ➤ Updated *Figure 5.23: Front-Panel Pinhole Reset*. **Section 9** ➤ Updated *Table 9.5: Troubleshooting Procedure*. **Appendix A** ➤ Updated for firmware version R102-V0 for the SEL-FLR. ➤ Updated for firmware version R100-V1 for the SEL-FLT. ➤ Added notes to both R100-V1 and R100-V0 for the SEL-FLT. **Appendix C** ➤ Updated *Table C.4: Event Logs*.
20190212	**Section 1** ➤ Updated *Table 1.2: SEL-FLR Orderable Accessories*. **Appendix A** ➤ Updated for firmware version R101-V1.
20181220	➤ Initial version.

APPENDIX B

DNP3 Profile and Data Map

DNP3 Documentation

Object List

Table B.1 lists the objects and variations with supported function codes and qualifier codes available in the SEL-FLR. The list of supported objects conforms to the format laid out in the DNP specifications and includes both supported and unsupported objects. Those that are supported include the function and qualifier codes. The objects that are not supported are shown without any corresponding function and qualifier codes.

Table B.1 SEL-FLR DNP Object List (Sheet 1 of 4)

Object			Request (supported)		Response (may generate)	
Obj	Var	Description	Func. Codes (dec)	Qual. Codes (hex)	Func. Codes (dec)	Qual. Codes (hex)
1	0	Binary Input—All Variations	1	0, 1, 6, 7, 8, 17, 28		
1	1	Binary Input	1	0, 1, 6, 7, 8, 17, 28	129	0, 1, 17, 28
1	2[a]	Binary Input with Status	1	0, 1, 6, 7, 8, 17, 28	129	0, 1, 17, 28
2	0	Binary Input Change—All Variations	1	6, 7, 8		
2	1	Binary Input Change Without Time	1	6, 7, 8	129	17, 28
2	2[a]	Binary Input Change With Time	1	6, 7, 8	129, 130	17, 28
2	3	Binary Input Change With Relative Time	1	6, 7, 8	129	17, 28
10	0	Binary Output—All Variations	1	0, 1, 6, 7, 8		
10	1	Binary Output				
10	2[a]	Binary Output Status	1	0, 1, 6, 7, 8	129	0, 1
12	0	Control Block—All Variations				
12	1	Control Relay Output Block	3, 4, 5, 6	17, 28	129	echo of request
12	2	Pattern Control Block	3, 4, 5, 6	7	129	echo of request
12	3	Pattern Mask	3, 4, 5, 6	0, 1	129	echo of request
20	0	Binary Counter—All Variations	1, 7, 8, 9, 10	0, 1, 6, 7, 8, 17, 18		
20	1[a]	32-Bit Binary Counter	1, 7, 8, 9, 10	0, 1, 6, 7, 8, 17, 18		
20	2	16-Bit Binary Counter	1, 7, 8, 9, 10	0, 1, 6, 7, 8, 17, 18		
20	3	32-Bit Delta Counter				
20	4	16-Bit Delta Counter				
20	5	32-Bit Binary Counter Without Flag	1, 7, 8, 9, 10	0, 1, 6, 7, 8, 17, 18	129	0, 1, 17, 28
20	6	16-Bit Binary Counter Without Flag	1, 7, 8, 9, 10	0, 1, 6, 7, 8, 17, 18	129	0, 1, 17, 28
20	7	32-Bit Delta Counter Without Flag				

Table B.1 SEL-FLR DNP Object List (Sheet 2 of 4)

Object			Request (supported)		Response (may generate)	
Obj	Var	Description	Func. Codes (dec)	Qual. Codes (hex)	Func. Codes (dec)	Qual. Codes (hex)
20	8	16-Bit Delta Counter Without Flag				
21	0	Frozen Counter—All Variations				
21	1	32-Bit Frozen Counter				
21	2	16-Bit Frozen Counter				
21	3	32-Bit Frozen Delta Counter				
21	4	16-Bit Frozen Delta Counter				
21	5	32-Bit Frozen Counter With Time of Freeze				
21	6	16-Bit Frozen Counter With Time of Freeze				
21	7	32-Bit Frozen Delta Counter With Time of Freeze				
21	8	16-Bit Frozen Delta Counter With Time of Freeze				
21	9	32-Bit Frozen Counter Without Flag				
21	10	16-Bit Frozen Counter Without Flag				
21	11	32-Bit Frozen Delta Counter Without Flag				
21	12	16-Bit Frozen Delta Counter Without Flag				
22	0	Counter Change Event—All Variations	1	6, 7, 8		
22	1	32-Bit Counter Change Event Without Time	1	6, 7, 8	129	17, 28
22	2	16-Bit Counter Change Event Without Time	1	6, 7, 8	129, 130	17, 28
22	3	32-Bit Delta Counter Change Event Without Time				
22	4	16-Bit Delta Counter Change Event Without Time				
22	5[a]	32-Bit Counter Change Event With Time	1	6, 7, 8	129	17, 28
22	6	16-Bit Counter Change Event With Time	1	6, 7, 8	129	17, 28
22	7	32-Bit Delta Counter Change Event With Time				
22	8	16-Bit Delta Counter Change Event With Time				
23	0	Frozen Counter Event—All Variations				
23	1	32-Bit Frozen Counter Event Without Time				
23	2	16-Bit Frozen Counter Event Without Time				
23	3	32-Bit Frozen Delta Counter Event Without Time				
23	4	16-Bit Frozen Delta Counter Event Without Time				
23	5	32-Bit Frozen Counter Event With Time				
23	6	16-Bit Frozen Counter Event With Time				
23	7	32-Bit Frozen Delta Counter Event With Time				
23	8	16-Bit Frozen Delta Counter Event With Time				
30	0	Analog Input—All Variations	1	0, 1, 6, 7, 8, 17, 28		
30	1	32-Bit Analog Input	1	0, 1, 6, 7, 8, 17, 28	129	0, 1, 7, 8
30	2	16-Bit Analog Input	1	0, 1, 6, 7, 8, 17, 28	129	0, 1, 7, 8
30	3	32-Bit Analog Input Without Flag	1	0, 1, 6, 7, 8	129	0, 1, 7, 8
30	4	16-Bit Analog Input Without Flag	1	0, 1, 6, 7, 8	129	0, 1, 7, 8
30	5[a]	Single-Precision Floating-Point Analog Input With Flag	1	0, 1, 6, 7, 8	129	0, 1, 7, 8

Table B.1 SEL-FLR DNP Object List (Sheet 3 of 4)

Object			Request (supported)		Response (may generate)	
Obj	Var	Description	Func. Codes (dec)	Qual. Codes (hex)	Func. Codes (dec)	Qual. Codes (hex)
30	6	Double-Precision Floating-Point Analog Input With Flag	1	0, 1, 6, 7, 8	129	0, 1, 7, 8
31	0	Frozen Analog Input—All Variations				
31	1	32-Bit Frozen Analog Input				
31	2	16-Bit Frozen Analog Input				
31	3	32-Bit Frozen Analog Input With Time of Freeze				
31	4	16-Bit Frozen Analog Input With Time of Freeze				
31	5	32-Bit Frozen Analog Input Without Flag				
31	6	16-Bit Frozen Analog Input Without Flag				
32	0	Analog Change Event—All Variations	1	6, 7, 8		
32	1	32-Bit Analog Change Event Without Time	1	6, 7, 8	129	17, 28
32	2	16-Bit Analog Change Event Without Time	1	6, 7, 8	129, 130	17, 28
32	3	32-Bit Analog Change Event With Time	1	6, 7, 8	129	17, 28
32	4	16-Bit Analog Change Event With Time	1	6, 7, 8	129	17, 28
32	5[a]	Single-Precision Floating-Point Analog Change Event Without Time	1	0, 1, 6, 7, 8, 17, 28	129	0, 1, 7, 8
32	6	Double-Precision Floating-Point Analog Change Event Without Time	1	0, 1, 6, 7, 8, 17, 28	129	0, 1, 7, 8
33	0	Frozen Analog Event—All Variations				
33	1	32-Bit Frozen Analog Event Without Time				
33	2	16-Bit Frozen Analog Event Without Time				
33	3	32-Bit Frozen Analog Event With Time				
33	4	16-Bit Frozen Analog Event With Time				
34	0	Analog Input Deadband—All Variations	1	0, 1, 6, 7, 8, 17, 28		
34	1	16-Bit Analog Input Deadband	1	0, 1, 6, 7, 8, 17, 28	129	0, 1, 17, 28
34	2	32-Bit Analog Input Deadband	1	0, 1, 6, 7, 8, 17, 28	129	0, 1, 17, 28
34	3	Single-Precision Floating-Point Analog Input Deadband	1	0, 1, 6, 7, 8, 17, 28	129	0, 1, 17, 28
40	0	Analog Output Status—All Variations	1	0, 1, 6, 7, 8		
40	1	32-Bit Analog Output Status	1	0, 1, 6, 7, 8	129	0, 1, 17, 28
40	2[a]	16-Bit Analog Output Status	1	0, 1, 6, 7, 8	129	0, 1, 17, 28
40	3	Single-Precision Floating-Point Analog Output Status	1	0, 1, 6, 7, 8	129	0, 1, 17, 28
40	4	Double-Precision Floating-Point Analog Output Status	1	0, 1, 6, 7, 8	129	0, 1, 17, 28
41	0	Analog Output Block—All Variations				
41	1	32-Bit Analog Output Block	3, 4, 5, 6	17, 28	129	echo of request
41	2	16-Bit Analog Output Block	3, 4, 5, 6	17, 28	129	echo of request
41	3	Single-Precision Floating-Point Analog Output Block	3, 4, 5, 6	17, 28	129	echo of request
41	4	Double-Precision Floating-Point Analog Output Block	3, 4, 5, 6	17, 28	129	echo of request
50	0	Time and Date—All Variations				
50	1	Time and Date	1, 2	7, 8 index = 0	129	07, quantity = 1

Table B.1 SEL-FLR DNP Object List (Sheet 4 of 4)

Object			Request (supported)		Response (may generate)	
Obj	Var	Description	Func. Codes (dec)	Qual. Codes (hex)	Func. Codes (dec)	Qual. Codes (hex)
50	2	Time and Date With Interval				
50	3	Time and Date at Last Recorded Time	2	7 index = 0	129	
51	0	Time and Date CTO—All Variations				
51	1	Time and Date CTO			129	07, quantity = 1
51	2	Unsynchronized Time and Date CTO			129	07, quantity = 1
52	0	Time Delay—All Variations				
52	1	Time Delay Coarse				
52	2	Time Delay Fine			129	07, quantity = 1
60	0	All Classes of Data	1, 20, 21	6		
60	1	Class 0 Data	1	6		
60	2	Class 1 Data	1, 20, 21	6, 7, 8		
60	3	Class 2 Data	1, 20, 21	6, 7, 8		
60	4	Class 3 Data	1, 20, 21	6, 7, 8		
70	1	File Identifier				
80	1	Internal Indications	2	0, 1 index = 7		
81	1	Storage Object				
82	1	Device Profile				
83	1	Private Registration Object				
83	2	Private Registration Object Descriptor				
90	1	Application Identifier				
100	1	Short Floating Point				
100	2	Long Floating Point				
100	3	Extended Floating Point				
101	1	Small Packed Binary-Coded Decimal				
101	2	Medium Packed Binary-Coded Decimal				
101	3	Large Packed Binary-Coded Decimal				
112	All	Virtual Terminal Output Block	2	6		
113	All	Virtual Terminal Event Data	2	6	129, 130	17, 28
N/A		No Object Required for the Following Function Codes: 13 cold start 14 warm start 23 delay measurement	13, 14, 23			

[a] Default variation.

Default Data Maps
SEL-FLR

Table B.2 shows the SEL-FLR default DNP3 data map. The default data map is automatically generated and is initialized to the default values.

NOTE: Time stamps (date and time) are in UTC time.

Table B.2 SEL-FLR Default DNP3 Data Map (Sheet 1 of 2)

Index	Type	Label	Description
Binary Inputs (Objects 01, 02)			
0	01, 02	FLR_ALARM	Alarm
1	01, 02	FLR_ENABLED	SEL-FLR is enabled
2	01, 02	FLR_ETHF_LINK_DET	EthF link detected
3	01, 02	FLR_ETHF_LINK_EN	EthF link enabled
4	01, 02	FLR_ETH1_LINK_DET	Eth1 link detected
5	01, 02	FLR_ETH1_LINK_EN	Eth1 link enabled
6	01, 02	FLR_ETH2_LINK_DET	Eth2 link detected
7	01, 02	FLR_ETH2_LINK_EN	Eth2 link enabled
8	01, 02	RESERVED	—
9	01, 02	RESERVED	—
10	01, 02	RESERVED	—
11	01, 02	RESERVED	—
12	01, 02	RESERVED	—
13	01, 02	RESERVED	—
14	01, 02	RESERVED	—
15	01, 02	RESERVED	—
16	01, 02	RESERVED	—
17	01, 02	RESERVED	—
18	01, 02	RESERVED	—
19	01, 02	RESERVED	—
20	01, 02	RESERVED	—
21	01, 02	RESERVED	—
22	01, 02	RESERVED	—
23	01, 02	RESERVED	—
24	01, 02	RESERVED	—
25	01, 02	RESERVED	—
26	01, 02	RESERVED	—
27	01, 02	RESERVED	—
28	01, 02	RESERVED	—
29	01, 02	RESERVED	—
30	01, 02	RESERVED	—
Binary Outputs (Objects 10, 12)			
0	10, 12	RESERVED	—
1	10, 12	RESERVED	—

Table B.2 SEL-FLR Default DNP3 Data Map (Sheet 2 of 2)

Index	Type	Label	Description
2	10, 12	RESERVED	—
3	10, 12	RESERVED	—
Analog Inputs (Objects 30, 32)			
0	30, 32, 34	FLR_FIRM_VER	Firmware version number
1	30, 32, 34	FLR_FIRM_POINT_VER	Firmware point release number
2	30, 32, 34	FLR_TEMP	Temperature
3	30, 32, 34	RESERVED	—
4	30, 32, 34	RESERVED	—
5	30, 32, 34	RESERVED	—
6	30, 32, 34	RESERVED	—
7	30, 32, 34	RESERVED	—
8	30, 32, 34	RESERVED	—
9	30, 32, 34	RESERVED	—
10	30, 32, 34	RESERVED	—
11	30, 32, 34	RESERVED	—
12	30, 32, 34	RESERVED	—
13	30, 32, 34	RESERVED	—
14	30, 32, 34	RESERVED	—
15	30, 32, 34	RESERVED	—
16	30, 32, 34	RESERVED	—

Radio FLR900

Table B.3 shows the SEL-FLR 900 MHz Radio Module default DNP3 data map. The default data map is automatically generated and is initialized to the default values.

Table B.3 Radio FLR900 Default DNP3 Data Map (Sheet 1 of 2)

Index	Type	Label	Description
Binary Inputs (Objects 01, 02)			
0	01, 02	RADIO_FLR900_NET_EN	Radio module network enable
1	01, 02	RADIO_FLR_NET_ISSUE	Radio module network issue
2	01, 02	RADIO_FLR900_RSSI_ALM	One joined SEL-FLT RSSI value is below –95 dBm
3	01, 02	RESERVED	—
4	01, 02	RESERVED	—
5	01, 02	RESERVED	—
6	01, 02	RESERVED	—
7	01, 02	RESERVED	—
8	01, 02	RESERVED	—
9	01, 02	RESERVED	—
10	01, 02	RESERVED	—
11	01, 02	RESERVED	—

Table B.3 Radio FLR900 Default DNP3 Data Map (Sheet 2 of 2)

Index	Type	Label	Description
12	01, 02	RESERVED	—
13	01, 02	RESERVED	—
Analog Inputs (Objects 30, 32)			
0	30, 32, 34	RADIO_FLR900_CHANNEL_NUM	Radio module channel
1	30, 32, 34	RADIO_FLR900_NUM_FLT_WHITELISTED	Number of whitelisted SEL-FLT devices
2	30, 32, 34	RADIO_FLR900_NUM_FLT_JOINED	Number of joined SEL-FLT devices
3	30, 32, 34	RESERVED	—
4	30, 32, 34	RESERVED	—
5	30, 32, 34	RESERVED	—
6	30, 32, 34	RESERVED	—
7	30, 32, 34	RESERVED	—
8	30, 32, 34	RESERVED	—
9	30, 32, 34	RESERVED	—
10	30, 32, 34	RESERVED	—
11	30, 32, 34	RESERVED	—
12	30, 32, 34	RESERVED	—

SEL-FLT

Table B.4 shows the SEL-FLT default DNP3 data map. The default data map is automatically generated and is initialized to the default values. The Device Address of the reporting SEL-FLT (which can be found on the product label) is included as a prefix on each DNP data point label.

Table B.4 SEL-FLT Default DNP3 Data Map (Sheet 1 of 3)

Index	Type	Label[a]	Description
Binary Inputs (Objects 01, 02)			
0	01, 02	*[DevAddr]*_FLT_ARM	Armed for Faults status
1	01, 02	*[DevAddr]*_DISPLAY	LED Display status
2	01, 02	*[DevAddr]*_FLASH_ERR	Flash Error alarm
3	01, 02	*[DevAddr]*_RAM_ERR	RAM Error alarm
4	01, 02	*[DevAddr]*_LOW_RECHARGE	Low Rechargeable Battery alarm
5	01, 02	*[DevAddr]*_CRT_RECHARGE	Critical Rechargeable Battery alarm (upcoming communications interruption)
6	01, 02	*[DevAddr]*_LOW_BATT	Low Non-Rechargeable Battery alarm
7	01, 02	*[DevAddr]*_LOW_PWR_HVST	Low Power Harvesting alarm
8	01, 02	*[DevAddr]*_COOR_ALRM	Coordination Alarm status
9	01, 02	*[DevAddr]*_FLT_STIM	Fault Stimulus status
10	01, 02	*[DevAddr]*_PERM_FLT	Permanent Fault status
11	01, 02	*[DevAddr]*_MOM_FLT	Momentary Fault status
12	01, 02	*[DevAddr]*_DIST	Disturbance status
13	01, 02	*[DevAddr]*_PERM_LOC	Permanent Loss-of-Current status
14	01, 02	*[DevAddr]*_MOM_LOC	Momentary Loss-of-Current status

Table B.4 SEL-FLT Default DNP3 Data Map (Sheet 2 of 3)

Index	Type	Label[a]	Description
15	01, 02	RESERVED	—
16	01, 02	RESERVED	—
17	01, 02	RESERVED	—
18	01, 02	RESERVED	—
19	01, 02	RESERVED	—
20	01, 02	RESERVED	—
21	01, 02	RESERVED	—
22	01, 02	RESERVED	—
23	01, 02	RESERVED	—
24	01, 02	RESERVED	—
Binary Outputs (Objects 10, 12)			
0	10, 12	RESERVED	—
1	10, 12	RESERVED	—
2	10, 12	RESERVED	—
Counter Inputs (Objects 20, 22)			
0	20, 22	*[DevAddr]*_PERM_FLT_STAT	Permanent fault statistic
1	20, 22	*[DevAddr]*_MOM_FLT_STAT	Momentary fault statistic
2	20, 22	*[DevAddr]*_DIST_STAT	Disturbance statistic
3	20, 22	*[DevAddr]*_COOR_ALRM_STAT	Coordination alarm statistic
4	20, 22	*[DevAddr]*_PERM_LOC_STAT	Permanent loss-of-current statistic
5	20, 22	*[DevAddr]*_MOM_LOC_STAT	Momentary loss-of-current statistic
6	20, 22	*[DevAddr]*_FLT_STIM_STAT	Fault stimulus statistic
7	20, 22	RESERVED	—
8	20, 22	RESERVED	—
9	20, 22	RESERVED	—
10	20, 22	RESERVED	—
11	20, 22	RESERVED	—
12	20, 22	RESERVED	—
Analog Inputs (Objects 30, 32)			
0	30, 32, 34	*[DevAddr]*_BACKUP_BATT_V	Non-rechargeable battery voltage
1	30, 32, 34	*[DevAddr]*_FIRM_VER	Firmware version number
2	30, 32, 34	*[DevAddr]*_FIRM_POINT_VER	Firmware point release number
3	30, 32, 34	*[DevAddr]*_SUI_AVG_LOAD	Short update average load
4	30, 32, 34	*[DevAddr]*_SUI_PEAK_LOAD	Short update peak load
5	30, 32, 34	*[DevAddr]*_LUI_AVG_LOAD	Long update average load
6	30, 32, 34	*[DevAddr]*_LUI_PEAK_LOAD	Long update peak load
7	30, 32, 34	*[DevAddr]*_FLT_MAG	Fault magnitude
8	30, 32, 34	*[DevAddr]*_FLT_RSSI	Device RSSI value
9	30, 32, 34	*[DevAddr]*_FLT_PER	Device packet error rate
10	30, 32, 34	RESERVED	—
11	30, 32, 34	RESERVED	—

Table B.4 SEL-FLT Default DNP3 Data Map (Sheet 3 of 3)

Index	Type	Label[a]	Description
12	30, 32, 34	RESERVED	—
13	30, 32, 34	RESERVED	—
14	30, 32, 34	RESERVED	—
15	30, 32, 34	RESERVED	—
16	30, 32, 34	RESERVED	—
17	30, 32, 34	RESERVED	—
18	30, 32, 34	RESERVED	—

[a] *[DevAddr]* will be replaced with the Device Address of the reporting SEL-FLT device.

This page intentionally left blank

APPENDIX C

Syslog

Introduction

The Syslog Protocol, defined in RFC 3164, provides a transport mechanism by which a device can send system event notification messages across IP networks to remote Syslog servers. Syslog is commonly used to send system logs such as security events, system events, and status messages useful in troubleshooting, auditing, and event investigations. The Syslog packet size is limited to 1024 bytes and is formatted into three parts: PRI, HEADER, and MSG.

1. **PRI:** The priority part of a Syslog packet is a number enclosed in angle brackets that represents both the facility and severity of the message. The priority value is calculated by multiplying the facility numerical code by 8 and adding the numerical value of the severity. For example, a kernel message (facility = 0) with a severity of Emergency (severity = 0) would have a priority of 0, while a "local use 4" message (facility = 20) with a severity of Notice (severity = 5) would have a priority value of 165. In the PRI part of the Syslog message, these values would be placed between the angle brackets as <0> and <165>, respectively.

   The severity code (*Table C.1*) is a number indicative of message importance.

Table C.1 Syslog Message Severities

Numerical Code	Severity
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

The facility code (*Table C.2*) defines the application group from which the message originated.

Table C.2 Syslog Message Facilities (Sheet 1 of 2)

Numerical Code	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons

Table C.2 Syslog Message Facilities (Sheet 2 of 2)

Numerical Code	Facility
4	Security/authorization messages[a]
5	Messages generated internally by Syslog Protocol
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon[b]
10	Security/authorization messages[a]
11	FTP daemon
12	NTP subsystem
13	Log audit[a]
14	Log audit[a]
15	Clock daemon[b]
16	Local use 0 (local 0)
17	Local use 1 (local 1)
18	Local use 2 (local 2)
19	Local use 3 (local 3)
20	Local use 4 (local 4)
21	Local use 5 (local 5)
22	Local use 6 (local 6)
23	Local use 7 (local 7)

[a] Various operating systems have been found to use Facilities 4, 10, 13, and 14 for security/authorization, audit, and alert messages that seem to be similar.

[b] Various operating systems have been found to use both Facilities 9 and 15 for clock (cron/at) messages. Source: www.faqs.org/rfcs/rfc3164.html

2. **HEADER:** The header of a Syslog packet contains the time stamp and the source of the message. The IP address or the hostname defines the source of the message. Time stamps are based on the time at the originating host, so it is critical to have time synchronized across devices for the entire network to accurately perform log analysis and event correlation.
3. **MSG:** The message part of a Syslog packet contains the source program that triggered the message and the human-readable body of the message.

A sample Syslog message follows. This particular message shows an invalid login attempt on July 09, 2009, at 08:17:29 to "myhostname" from the IP address 192.168.1.1. The priority of this message is 37.

```
<37>Jul 09 2009 08:17:29 myhostname Login: Login to web: failed
from 192.168.1.1
```

The Syslog message has been divided into each respective part, as shown in *Table C.3*.

Table C.3 Example Syslog Message Components

PRI	HEADER	MSG
<37>	Jul 09 2009 08:17:29 myhostname	Login: Login to web: failed from 192.168.1.1

Remote Syslog Servers

Syslog messages are stored locally and optionally sent to remote Syslog servers. The local buffers are circular in nature, with newer messages overwriting older messages after the buffer fills. Support for multiple remote Syslog servers provides the added benefits of centralized logging, including larger storage capacity, centralized event analysis and correlation, and archival event logs. In *Figure C.1*, remote devices are configured to send Syslog messages to the remote Syslog server through the use of a secure network or a nonsecured network with a VPN tunnel. In this example, Syslog-compatible devices can send logs to the central Syslog server for centralized logging, reporting, and event correlation. The Syslog Protocol uses User Datagram Protocol (UDP) Port 514 to send Syslog messages to remote Syslog servers.

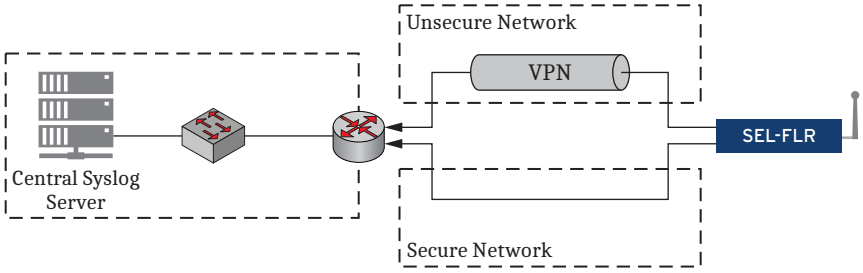


Figure C.1 Central Syslog Server

Open-Source Syslog Servers

Most Linux and UNIX distributions include a native Syslog server that can be used for a central Syslog server solution. Syslog-ng (syslog-ng.com) is also an excellent solution that, if not already included in your distribution, can be used for added functionality. Syslog server solutions for Microsoft Windows are typically commercially available or have limited feature sets if offered at no charge.

SEL-FLR Event Logs

The SEL-FLR records and time-stamps all events in the Syslog format consistent with the Syslog description from RFC 3164. *Table C.4* lists all of the events that the SEL-FLR logs and the record the clock generates with each event.

Log messages may contain words or phrases in brackets such as {0}. This notation indicates a variable that the SEL-FLR replaces with the value being logged. For example, the SEL-FLR would replace the {0} in the Syslog message `User account {0} locked out due to consecutive failed login attempts` with the actual username that was locked out.

Table C.4 Event Logs (Sheet 1 of 5)

Message	Tag	Severity	Facility	Alarm
Device factory reset initiated by user {userName} with role {roleName} from IP Address {ipAddress}	DeviceReset	Notice	SecurityOrAuthorization-Messages1	None
FLT_{DevAddress} could not be authenticated.	FltNetwork	Warning	SecurityOrAuthorization-Messages1	None

Table C.4 Event Logs (Sheet 2 of 5)

Message	Tag	Severity	Facility	Alarm
Unable to update password for {username}	SecurityManager	Informational	SecurityOrAuthorization-Messages2	None
Unable to authenticate user from IP address {ipAddress}	SecurityManager	Notice	SecurityOrAuthorization-Messages2	None
Authenticated user {username} in role {role} from IP address {ipAddress}	SecurityManager	Notice	SecurityOrAuthorization-Messages2	None
Invalid token presented to the rest interface IP address {ipAddress}	SecurityManager	Warning	SecurityOrAuthorization-Messages2	None
Denied permission for user {username} in role {role} from module {module} to {permissionsList}	SecurityManager	Warning	SecurityOrAuthorization-Messages2	None
Session for user {user} has ended	SecurityManager	Warning	SecurityOrAuthorization-Messages2	None
A firmware version downgrade is not compatible with the current firmware.	FirmwareUpgrade	Error	SystemDaemons	Minor
An error occurred with the restored database {error}	Persistence	Error	SystemDaemons	Minor
Database corruption prevented database upgrade. Please contact SEL for further assistance.	Persistence	Error	SystemDaemons	Minor
Database file accessed while locked	Persistence	Error	SystemDaemons	Minor
Failure: Flash	Diagnostics	Alert	SystemDaemons	Major
Failure: HMI	Diagnostics	Alert	SystemDaemons	Major
Failure: Primary Device Operations Inhibited	Diagnostics	Alert	SystemDaemons	Major
Failure: Radio Module FlrRadio900 communications.	FltNetwork	Alert	SystemDaemons	Major
Failure: RAM	Diagnostics	Alert	SystemDaemons	Major
Failure: Real Time Clock	Diagnostics	Alert	SystemDaemons	Major
Firmware upgrade from {oldVersion} to {newVersion} failed at step {failedStep} of {failedStepCount}.	FirmwareUpgrade	Critical	SystemDaemons	Major
Firmware upgrade from {oldVersion} to {newVersion} failed for FLT_{DevAddress}.	FltNetwork	Critical	SystemDaemons	Major
FLT Network firmware upgrade completed with errors. Please contact Schweitzer Engineering Laboratories, Inc. for assistance.	FltNetwork	Critical	SystemDaemons	Major
FLT_{DevAddress} Failure: Flash	FaultedCircuitIndicator	Error	SystemDaemons	Minor
FLT_{DevAddress} Failure: Low Non-Rechargeable Battery	FaultedCircuitIndicator	Error	SystemDaemons	Minor
FLT_{DevAddress} Failure: RAM	FaultedCircuitIndicator	Error	SystemDaemons	Minor
Insufficient disk space for data storage. Free additional disk space.	Persistence	Critical	SystemDaemons	Major
Local event storage contains >= {unackdPercent} unacknowledged events.	LocalEventStore	Critical	SystemDaemons	Major
Okay: Flash	Diagnostics	Alert	SystemDaemons	Major[a]
Okay: HMI	Diagnostics	Error	SystemDaemons	Minor[a]
Okay: Radio Module FlrRadio900 communications.	FltNetwork	Alert	SystemDaemons	Major[a]
Okay: RAM	Diagnostics	Alert	SystemDaemons	Major[a]
Okay: Real Time Clock	Diagnostics	Alert	SystemDaemons	Major[a]

Table C.4 Event Logs (Sheet 3 of 5)

Message	Tag	Severity	Facility	Alarm
Reverted to fallback firmware version {firmwareVersion}. Previous device settings are in effect. Please contact Schweitzer Engineering Laboratories, Inc. for assistance.	FirmwareUpgrade	Critical	SystemDaemons	Major
Selected database was corrupt. Now attempting to restore previous database	Persistence	Error	SystemDaemons	Minor
The current database was generated by {appName} version {dbVersion}. The current {appName} version is {currentVersion}. Please upgrade the {appName} to the version the database was generated with or higher.	Persistence	Error	SystemDaemons	Minor
The database was created by {dbsApp}. It is not compatible with {runningApp}.	Persistence	Error	SystemDaemons	Minor
The firmware image is corrupted.	FirmwareUpgrade	Error	SystemDaemons	Minor
The FLT Network firmware version downgrade is not compatible with the current firmware on FLT_{DevAddress}.	FltNetwork	Error	SystemDaemons	Minor
The rechargeable battery in FLT_{DevAddress} is critically-low.	FaultedCircuitIndicator	Error	SystemDaemons	Minor
Created new database	Persistence	Informational	SystemDaemons	None
Firmware upgrade from {oldVersion} to {newVersion} started for FLT_{DevAddress}.	FltNetwork	Informational	SystemDaemons	None
Firmware upgrade from {oldVersion} to {newVersion} succeeded for FLT_{DevAddress}.	FltNetwork	Informational	SystemDaemons	None
FLT Network firmware upgrade started.	FltNetwork	Informational	SystemDaemons	None
FLT Network firmware upgrade completed successfully.	FltNetwork	Informational	SystemDaemons	None
Restored database	Persistence	Informational	SystemDaemons	None
FLT_{DevAddress} Okay: Non-Rechargeable Battery	FaultedCircuitIndicator	Notice	SystemDaemons	None
Okay: Device Enabled	Diagnostics	Notice	SystemDaemons	None
Local event storage contains <= {unackdPercent} unacknowledged events.	LocalEventStore	Notice	SystemDaemons	None
FLT_{DevAddress} Okay: Flash	FaultedCircuitIndicator	Notice	SystemDaemons	None
FLT_{DevAddress} Okay: RAM	FaultedCircuitIndicator	Notice	SystemDaemons	None
{displayName} changed link state to down.	BasicNetworkInterfaces	Notice	SystemDaemons	None
{displayName} changed link state to up.	BasicNetworkInterfaces	Notice	SystemDaemons	None
FLT_{DevAddress}: Line power harvesting restored.	FaultedCircuitIndicator	Notice	SystemDaemons	None
FLT_{DevAddress} Okay: Rechargeable Battery	FaultedCircuitIndicator	Notice	SystemDaemons	None
The rechargeable battery in FLT_{DevAddress} is charged.	FaultedCircuitIndicator	Warning	SystemDaemons	None
Local event storage contains >= {unackdPercent} unacknowledged events.	LocalEventStore	Warning	SystemDaemons	None
FLT_{DevAddress}: Line power harvesting failed.	FaultedCircuitIndicator	Warning	SystemDaemons	None

Table C.4 Event Logs (Sheet 4 of 5)

Message	Tag	Severity	Facility	Alarm
FLT_{DevAddress} Failure: Low Rechargeable Battery	FaultedCircuitIndicator	Warning	SystemDaemons	None
Firmware upgrade from {oldVersion} to {newVersion} succeeded.	FirmwareUpgrade	Warning	SystemDaemons	None
Device reset because of {reason}	DeviceReset	Warning	SystemDaemons	None
Failure: Real Time Clock Battery	Diagnostics	Warning	SystemDaemons	None
Okay: Real Time Clock Battery	Diagnostics	Warning	SystemDaemons	None
Device factory default reset initiated via pinhole reset button.	FlrDataShim	Alert	UserLevelMessages	Major
Device management port reset initiated via pinhole reset button.	FlrDataShim	Alert	UserLevelMessages	Major
The SEL-FLT firmware image is corrupted.	FltNetwork	Error	UserLevelMessages	Minor
Device reboot initiated by user {userName} with role {roleName} from IP Address {ipAddress}	DeviceReset	Error	UserLevelMessages	Minor
Failed to synchronize settings with FLT_{DevAddress}.	FltNetwork	Error	UserLevelMessages	Minor
Commissioning succeeded	CommissioningManager	Informational	UserLevelMessages	None
Settings successfully synchronized with FLT_{DevAddress}.	FltNetwork	Informational	UserLevelMessages	None
User {userName} with role {roleName} from {ipAddress} acknowledged all local events.	LocalEventStore	Notice	UserLevelMessages	None
User {username} uploaded certificate {thumbprint} for {certificatePurpose}.	TrustAuthority	Notice	UserLevelMessages	None
Updated event category {eventCategory}	EventBus	Notice	UserLevelMessages	None
FLT_{DevAddress}: Current restored.	FaultedCircuitIndicator	Notice	UserLevelMessages	None
FLT_{DevAddress}: Fault stimulus present.	FaultedCircuitIndicator	Notice	UserLevelMessages	None
FLT_{DevAddress} failed to join.	FltNetwork	Notice	UserLevelMessages	None
FLT_{DevAddress} joined successfully.	FltNetwork	Notice	UserLevelMessages	None
FLT_{DevAddress} unjoined from network.	FltNetwork	Notice	UserLevelMessages	None
FLT Network firmware upgrade was canceled by user {username} with role {role} from IP address {ipAddress}.	FltNetwork	Notice	UserLevelMessages	None
FLT Network firmware upgrade was scheduled from {startTime} to {endTime} by user {username} with role {role} from IP address {ipAddress}.	FltNetwork	Notice	UserLevelMessages	None
User {user} with role {role} modified configuration object {id} from IP address {ipAddress}	DataBroker	Notice	UserLevelMessages	None
Log delivery was not confirmed to behavior {behaviorType} for event with id {monotonicId}	EventBus	Notice	UserLevelMessages	None
FLT_{DevAddress}: Disturbance detected.	FaultedCircuitIndicator	Notice	UserLevelMessages	None
FLT_{DevAddress}: Momentary fault detected.	FaultedCircuitIndicator	Notice	UserLevelMessages	None
FLT_{DevAddress}: Momentary loss of current detected.	FaultedCircuitIndicator	Notice	UserLevelMessages	None
FLT_{DevAddress}: Permanent fault detected.	FaultedCircuitIndicator	Notice	UserLevelMessages	None

Table C.4 Event Logs (Sheet 5 of 5)

Message	Tag	Severity	Facility	Alarm
FLT_{DevAddress}: Permanent loss of current detected.	FaultedCircuitIndicator	Notice	UserLevelMessages	None
Permission denied to user owned object {objectId} for user {username} in role {role} from module {module} to {permissionsList}	DataBroker	Notice	UserLevelMessages	None
Firmware upgrade was initiated by user {username} with role {role} from IP address {ipaddress}.	FirmwareUpgrade	Notice	UserLevelMessages	None
User {user} with role {role} and module {module} executed action {action} on {id} from IP address {ipAddress}	DataBroker	Notice	UserLevelMessages	None
User {user} with role {role} and module {module} executed unbound action {action} from IP address {ipAddress}	DataBroker	Notice	UserLevelMessages	None
User {user} with role {role} and module {module} failed to execute action {action} on {id} from IP address {ipAddress}	DataBroker	Notice	UserLevelMessages	None
User {user} with role {role} and module {module} failed to execute unbound action {action} from IP address {ipAddress}	DataBroker	Notice	UserLevelMessages	None
User {userName} with role {roleName} manually set the device system time.	ManualTime	Notice	UserLevelMessages	None
User {username} failed to import certificate for purpose {purpose}	TrustAuthority	Warning	UserLevelMessages	None
Certificate with common name {commonName} and thumbprint {thumbprint} internally {revokeState}	TrustAuthority	Warning	UserLevelMessages	None
User {username} revoked certificate {thumbprint}	TrustAuthority	Warning	UserLevelMessages	None
Commissioning failed	CommissioningManager	Warning	UserLevelMessages	None
FLT_{DevAddress}: Mis-Coordination detected.	FaultedCircuitIndicator	Warning	UserLevelMessages	None
Event storage capacity ({storageCapacity}) exceeded. Oldest {numberRemoved} events removed.	LocalEventStore	Warning	UserLevelMessages	None

[a] Indicates a self-clearing alarm.

This page intentionally left blank

APPENDIX D

Link Budget Analysis

Overview

A radio link budget accounts for all losses and gains in a radio link from the transmitter to the receiver. Link budget calculations are used to determine the amount of link margin available for a given radio link. The link budget includes five components: radio transmit power, antenna gains, cable and path losses, interference margin, and radio receiver sensitivity. For a reliable link, the receive power must be greater than the effective receive sensitivity. The link margin is the difference between received power and effective receive sensitivity. The goal of link budget calculation is to account for all of the system and path gains and losses to determine if an adequate link margin is available (see *Figure D.1*).

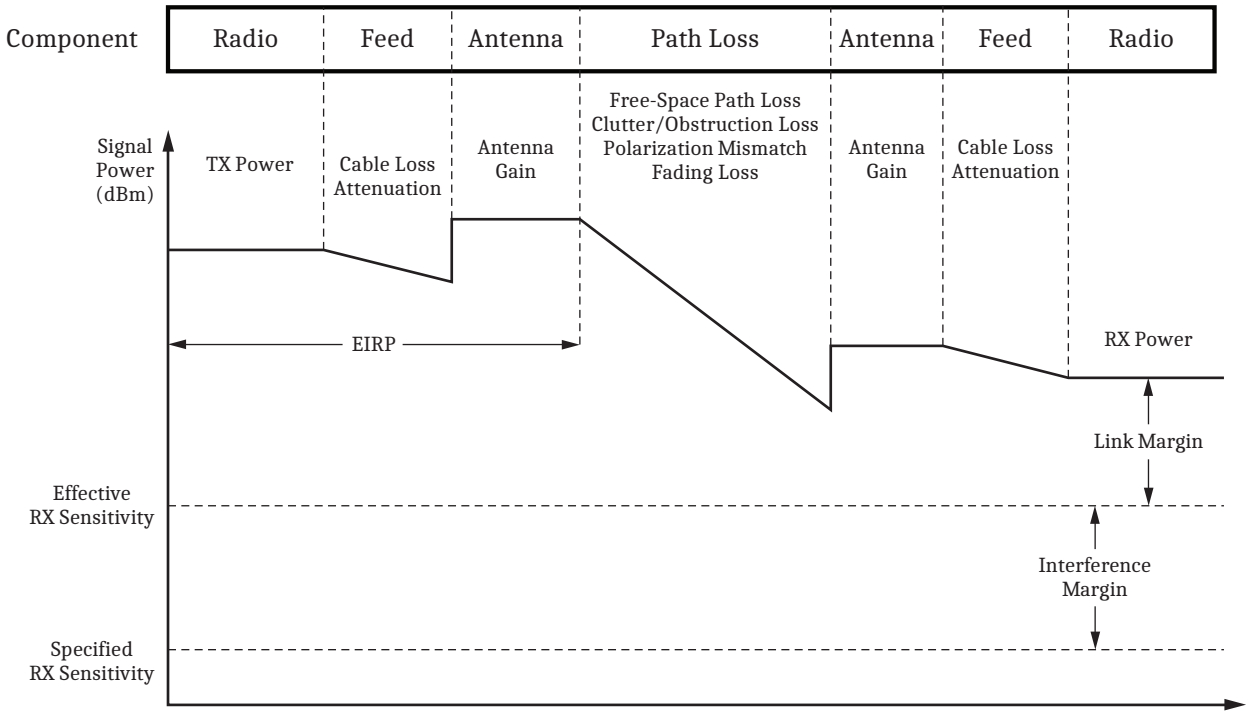


Figure D.1 Sample Link Budget

Transmitted and Radiated Power Requirements

FCC and IC regulations for 900 MHz ISM (industrial, scientific, and medical) band radios such as those used by the SEL-FLR and SEL-FLT place limits of +30 dBm (+27 dBm for Ecuador) on maximum radio transmit power and

+36 dBm (+30 dBm for Costa Rica) on maximum Effective Isotropic Radiated Power (EIRP). EIRP is a measure of the amount of power radiated from the main lobe of the transmitter antenna, and is calculated using *Equation D.1*.

$$\text{EIRP (dBm)} = \text{TX Power (dBm)} - \text{Line Loss (dB)} - \text{Attenuation (dB)} + \text{Antenna Gain (dBi)}$$

Equation D.1

The radio module in the SEL-FLT and SEL-FLR has a maximum transmitted power of +26 dBm, in compliance with FCC and IC requirements for 900 MHz ISM band devices. The SEL-FLT has a single integral antenna with an average gain of –4 dBi in the horizontal plane and a maximum of 0.8 dBi for regulatory calculations.

The SEL-FLR must be connected to an external antenna. The user must verify that the SEL-FLR does not exceed FCC and IC maximum EIRP limits when using the external antenna. In some instances, this may require that additional fixed attenuation be added between the radio and the antenna to comply with maximum EIRP requirements.

Using antenna choices from *Table D.2*, for example, the 7.15 dBi omnidirectional antenna with a line-feed loss of 1.95 dB (i.e., 12.24 m [50 ft] of LMR-400 cable; from *Table D.1*) results in an EIRP of 31.20 dBm, which is compliant with the FCC and IC regulations. However, using the 14.15 dBi Yagi antenna with the same feed line results in an EIRP of 38.20 dBm. This is not compliant and would require that additional fixed attenuation be placed between the radio and the antenna. If a 3 dB fixed attenuator is added to the feed, the EIRP would be 35.20 dBm, which would be compliant.

Table D.1 Cable Loss

Cable Type	3.05 m (10 ft)	12.24 m (50 ft)	30.48 m (100 ft)	91.44 m (300 ft)
LMR-400	0.39 dB	1.95 dB	3.9 dB	13.1 dB
0.5-inch Heliax	Do Not Use	1.15 dB	2.29 dB	6.87 dB
0.875-inch Heliax	Do Not Use	0.64 dB	1.28 dB	3.84 dB
1.25-inch Heliax	Do Not Use	Do Not Use	0.95 dB	2.85 dB

NOTE: The SEL-FLR has been designed to operate with the antennas listed in *Table D.2*. Antennas not included in this list, or that have a gain greater than the same type of antenna found in the table are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

Table D.2 Antenna Gain[a]

SEL Part Number	Antenna Type	Gain
235-0003	Pole-Top, Low-Profile Omnidirectional	3 dBi
235-0232	Pole-Top, Vertical Omnidirectional	7.15 dBi
235-0233	Pole-Top, Vertical Omnidirectional	9.15 dBi
235-0234	Base Station, Vertical Omnidirectional	8.1 dBi
235-0221	Yagi, 3-Element	8.5 dBi
235-0220	Yagi, 5-Element	11.1 dBi
235-0222	Yagi, 11-Element	14.1 dBi

[a] Not certified for Brazil (model FLR-1006). Contact SEL for approved antenna models.

Path Loss

Path loss is attenuation of the transmitted signal as it propagates between the transmitter and the receiver. There can be multiple contributors to total path loss, including free-space path loss (FSPL), loss due to obstructions within the path of the radio signal, polarization mismatch between the transmitting and receiving antennas, and multi-path fading. Total path loss is calculated using *Equation D.2*. Loss due to obstructions, antenna polarization mismatch, and fading generally need to be estimated. All potential path loss factors should be included in the link budget calculation when determining link margin.

$$\text{Path Loss (dB)} = \text{FSPL (dB)} - \text{Obstruction Loss (dB)} + \text{Polarization Loss (dB)} - \text{Fading Loss (dB)}$$

Equation D.2

Free-Space Path Loss

Free-space path loss is calculated through the use of *Equation D.3*. *Table D.3* shows the 915 MHz free-space path loss for some example path distances.

$$\text{FSPL (dB)} = 32.45 + 20\log f\,(\text{MHz}) + 20\log d\,(\text{km})$$

Equation D.3

where:

f = frequency in MHz
d = distance in km

Table D.3 915 MHz Free-Space Path Loss Examples

Distance Between Antennas (d)	Free-Space Path Loss
300 m (1000 ft)	81 dB
1.6 km (1 mi)	96 dB
8 km (5 mi)	110 dB

Obstruction Loss

Path loss caused by obstructions needs to be factored into link budget calculations when there are obstructions within the first Fresnel zone of the radio link. The first Fresnel zone is an elliptical space surrounding the direct path between the transmitter and the receiver antennas, the perimeter of which is described by a total chord distance (d1 + d2) that is half a wavelength greater than the length of the direct path (d) between the transmitter and receiver antennas.

The maximum radius of the first Fresnel zone occurs at a point midway between the transmitting and receiving antennas, as shown in *Figure D.2*. *Equation D.4* shows how to calculate the radius of the Fresnel zone. For example, at 915 MHz with a distance of 300 m (1000 ft) between antennas, the Fresnel zone has a radius of 4.96 m (16.27 ft). *Table D.4* provides the Fresnel zone radius for some example path distances.

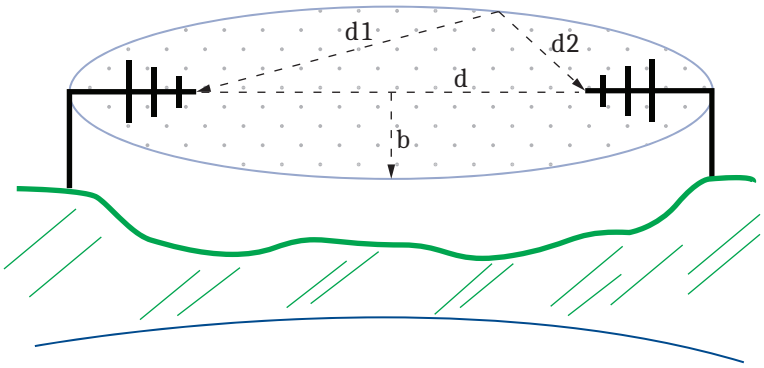


Figure D.2 Fresnel Zone

$$b = 547.7\sqrt{\frac{d}{4f}}$$

Equation D.4

where:

b = radius of the Fresnel zone in meters
d = distance between transmitter and receiver in kilometers
f = frequency transmitted in MHz

Table D.4 915 MHz Fresnel Zone Radius

Distance Between Antennas (d)	Fresnel Zone Radius (b)
300 m (1000 ft)	4.96 m (16.27 ft)
1.6 km (1 mi)	11.45 m (37.57 ft)
8 km (5 mi)	25.60 m (83.99 ft)

When you have a clear line of sight, with no obstructions within the first Fresnel zone of the radio link, no obstruction loss value is needed in the link budget calculation. Anything within the Fresnel zone (the ground, buildings, vegetation, etc.) will add obstruction loss to the link budget calculation. When more than 80 percent of the Fresnel zone radius is free of obstructions, 0–3 dB of loss can be added to the link budget to account for obstruction loss. When 50–80 percent of the Fresnel zone radius is free from obstructions, 6–12 dB of obstruction loss can be added to the link budget. When less than 50 percent of the Fresnel zone is free from obstruction, 12–20 dB of obstruction loss can be added to the link budget. When obstructions occur on the direct path between the transmitting and receiving antennas, more than 20 dB of obstruction loss may need to be added to the link budget.

Antenna Polarization Loss

Antenna polarization refers to the orientation of the e-field in the radiated RF signal. The omnidirectional antennas listed in *Table D.2* are all vertically polarized. The Yagi antennas are polarized in the direction of the short radiating elements of the antenna (either vertically or horizontally). For proper system operation, the transmitting and receiving antenna should be polarized in the same direction. When a radio signal propagates over long distances, it is possible for the polarization of the signal to rotate (due to interactions with the ground or obstructions in the path). When this occurs, the received signal polarization may not be aligned with the receiving antenna, which results in polarization mismatch loss.

A 45-degree rotation of signal polarization results in a 3 dB loss of received signal power. It is possible but unlikely for greater polarization loss to occur in an actual radio link.

Fading Loss

Multi-path fading occurs when the transmitted signal is reflected off surfaces that are not on the direct path between the transmitter and receiver. These reflected signal images combine with the direct path signal and add constructively or destructively depending on the phase of the reflected signal relative to the direct path signal. When a direct line-of-sight path exists between the transmitter and receiver, multi-path fading will generally be approximately 6–10 dB, in the presence of nearby reflective surfaces. When a direct line-of-sight path does not exist between the transmitter and receiver, multi-path fading can cause 20 dB or more of signal loss.

Interference Margin

The SEL-FLT/SEL-FLR system shares frequency spectrum with other services and FCC Part 15 (unlicensed) devices in ITU Region 2 (North, Central, and South America). Signals from other devices and services in the 900 MHz ISM band can cause interference at the receiver that degrades the receive sensitivity of the radio. The effective receive sensitivity of the radio is the signal level at which the radio can properly receive the desired signal in the presence of sustained interference.

Interference margin should be included in the link budget to account for the effect of interfering signals. The level of interference at a receiver can vary greatly depending on the number of other nearby devices and services operating in a given area. In isolated locations, there may be very little interference (0–6 dB of interference margin required). In suburban or urban environments, the level of interference can be substantial (6–20 dB of interference margin required).

Link Margin

The result of a link budget calculation is a determination of the link margin available for a given radio link. While it is possible for a radio link to work properly with 0 dB of link margin, it is undesirable to design a system with little or no link margin. Link budget calculations often rely on estimates of loss factors and interference levels and may not be accurate. In addition, over time, the conditions of the link may change, resulting in additional path loss or new sources of interference, which could render the link unreliable. In practice, allowing for 10–15 dB of link margin should result in a reliable link at installation and provide tolerance for changes over time. Use *Equation D.5*, *Equation D.6*, and *Equation D.7* to calculate link margin.

$$\text{RX Signal Strength (dBm)} = \text{TX Power (dBm)} - \text{Line Loss}_{FLR}\text{ (dBi)} - \text{Attenuation}_{FLR}\text{ (dB)} + \text{Antenna Gain}_{FLR}\text{ (dBi)} - \text{Path Loss (dB)} + \text{Antenna Gain}_{FLT}\text{ (dBi)} - \text{Line Loss}_{FLT}\text{ (dB)}$$

Equation D.5

$$\text{Effective RX Sensitivity (dBm)} = \text{RX Sensitivity (dBm)} - \text{Interference Margin (dBm)}$$

Equation D.6

$$\text{Link Margin (dB)} = \text{RX Signal Strength (dBm)} - \text{Effective RX Sensitivity (dBm)}$$

Equation D.7

Link Budget Calculation Example

The following example of a link budget calculation illustrates how loss factors and interference affect available link margin.

Example

The SEL-FLR antenna is mounted half-way up a utility pole and the SEL-FLT is located 400 m (0.25 mi) away. There is approximately 40 percent obstruction within the Fresnel zone. There is also another 900 MHz radio nearby that has moderate interference.

System

SEL-FLT/SEL-FLR Transmit Power: +26 dBm
SEL-FLT/SEL-FLR Receive Sensitivity: –102 dBm
SEL-FLT Antenna Gain: –4 dBi

SEL-FLR Antenna

Omnidirectional Antenna (SEL part number 235-0232): +7.15 dBi
3.05 m (10 ft) of LMR-400 Coaxial Cable: –0.39 dB
Radio Surge Protector (SEL part number 200-2004): –0.25 dB

Path

Obstruction Loss: –5 dB
Polarization Loss: 0 dB
Fading Loss: –6 dB
Interference Margin: –6 dB

SEL-FLR EIRP (*Equation D.1*)

$$\text{EIRP (dBm)} = +26\ \text{(dBm)} - 0.39\ \text{(dB)} - 0.25\ \text{(dB)} + 7.15\ \text{(dBi)}$$
$$\text{EIRP (dBm)} = 32.51\ \text{(dBm)}$$

Note: This is within the FCC and IC limits.

Free-Space Path Loss (*Equation D.3*)

$$\text{FSPL (dB)} = 32.45 + 20\log 915\ \text{(MHz)} + 20\log 0.4\ \text{(km)}$$
$$\text{FSPL (dB)} = -83.7\ \text{(dB)}$$

Path Loss (*Equation D.2*)

$$\text{Path Loss (dB)} = -83.7\ \text{(dB)} - 5\ \text{(dB)} + 0\ \text{(dB)} - 6\ \text{(dB)}$$
$$\text{Path Loss (dB)} = -94.7\ \text{(dB)}$$

Receive Signal Strength (*Equation D.5*)

RX Signal Strength (dBm) = +26 (dBm) – 0.39 (dBi) – 0.25 (dB) + 7.15 (dBi) – 94.7 (dB) – 4 (dBi) + 0 (dB)
RX Signal Strength (dBm) = –66.2 (dBm)

Effective Receive Sensitivity (*Equation D.6*)

Effective RX Sensitivity (dBm) = –102 (dBm) – (–6 (dB))
Effective RX Sensitivity (dBm) = –96 (dBm)

Link Margin (*Equation D.7*)

Link Margin (dB) = –66.2 (dBm) + 96 (dBm)
Link Margin (dB) = 29.8 (dB)

A link margin of 29.8 dB will provide sufficient coverage for this application.

This page intentionally left blank

APPENDIX E

X.509

Introduction

In cryptography, X.509 is an International Telecommunication Union standard for public-key infrastructure (PKI). X.509 specifies formats for public-key certificates and validation paths for authentication. The SEL-FLR uses X.509 certificates in the web server for secure device management and for IPsec authentication.

This appendix includes the following:

Symmetric-Key Cryptography

Symmetric-key cryptography, which has been used in various forms for thousands of years, uses a single key that both encrypts and decrypts the message. This key must be shared between the sender and receiver in advance. If the key cannot be shared securely, the confidentiality of any transmission encrypted with that key cannot be known.

Public-Key Cryptography

Public-key cryptography is distinguished by the use of asymmetric keys instead of the more traditional symmetric keys. Asymmetric keys are mathematically related so that whatever one key encrypts, the other key must be used to decrypt. There is no way to derive one key from knowledge of its paired key. These key pairs are known as public and private keys, as shown in *Figure E.1*. The private key must be kept secret, while the public key can be distributed freely. This allows for many methods of protecting and authorizing messages that are not possible with symmetric-key cryptography.

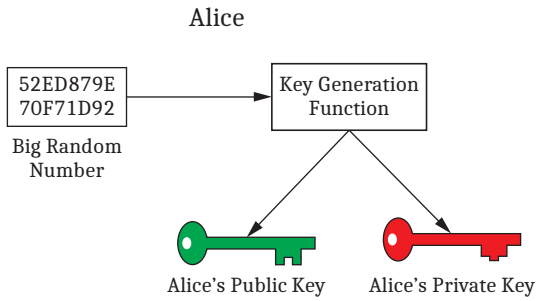


Figure E.1 Asymmetric Keys

In public-key cryptography, the encryption key is not the same as the decryption key. If a message is encrypted with the publicly known key, only the private key can be used to decrypt it, as shown in *Figure E.2*. This private key is known only to the owner of the key pair. Only the sender and the intended receiver will know the message, ensuring confidentiality.

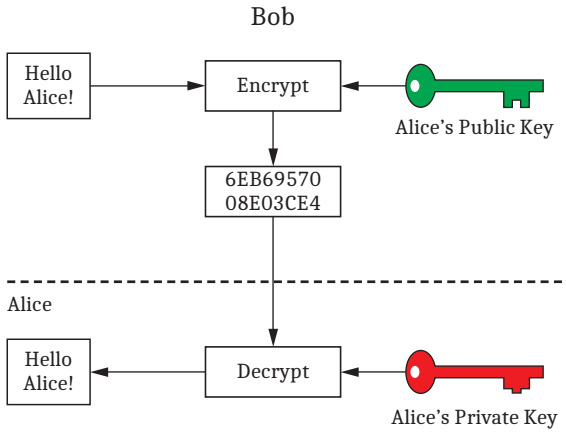


Figure E.2 Confidentiality With Asymmetric Keys

Public-key cryptography is much more computation intensive than symmetric-key cryptography. This makes it infeasible to send large amounts of data, or secure a series of transmissions, using this technology. Public-key cryptography offers confidentiality and the corresponding ability to exchange symmetric keys securely and confidentially. This is known as hybrid cryptography and is one way that IPsec uses public-key cryptography.

You can also use public-key cryptography for authentication. Do this by using a private key, rather than the public key, as the encryption key (as shown in *Figure E.3*). The public key you use to decrypt the message will identify the sender. This is known as an electronic signature.

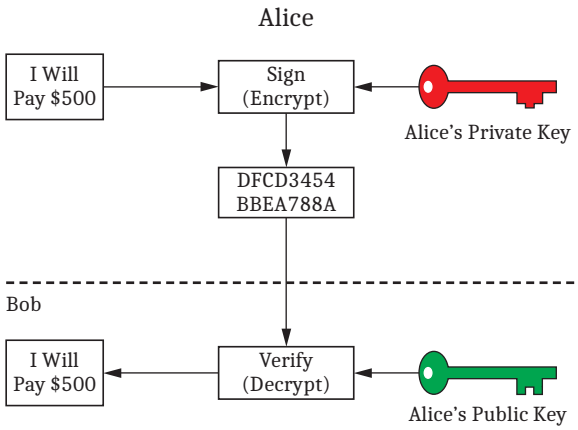


Figure E.3 Authentication With Asymmetric Keys

X.509 Certificates

Digital certificates, also known as public-key certificates, provide a formal method for associating pairs of asymmetric keys with their owners. You can use these electronic documents, through the use of digital signatures, to bind public keys to their owners.

Digital Signatures

A digital signature is a more formal method of authenticating data than an electronic signature. They can be compared to the wax seals that were placed on envelopes before email was available. To create a digital signature of data, you first compute a hash of the data to be signed and then encrypt that hash with the signer's private key. You then attach this signature to the data to be signed. To verify the authenticity of the data, the receiver's system first separates data and signature. The receiver computes their own hash of the data and then uses the issuer's public key to decrypt the signature (i.e., the sender's encrypted hash). The two hashes are then compared, and if they match (as shown in *Figure E.4*), the data are verified as authentic.

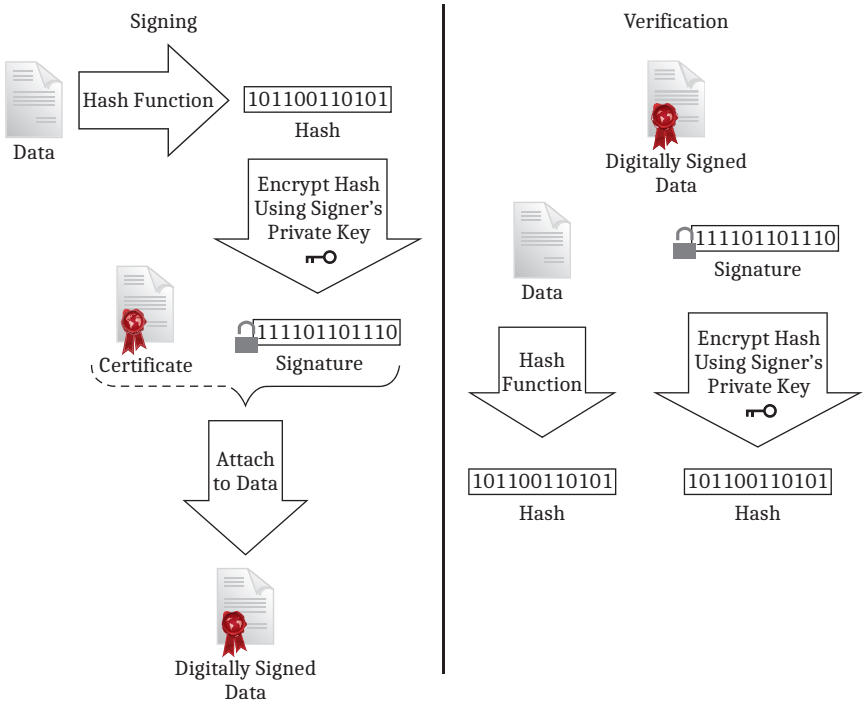


Figure E.4 Digital Signatures

Public-Key Infrastructure

One of three common uses for digital certificates is in a public-key infrastructure (PKI). PKI is a formal, hierarchical system where a digital certificate may contain the signature of one or a chain of more trusted certificate issuers. At the top of the PKI hierarchy is the most trusted certificate, a root certificate. A root certificate is self-signed, highly protected, and should only be used to sign Certificate Authority (CA) certificates. Root certificates have to be manually made trusted by a system administrator, or they must be included by the software vendor in a cache of trusted root certificates. Most modern operating systems, such as Microsoft Windows, preload a collection of root certificates for commonly used (and trusted) certificate authorities (e.g., VeriSign, Thawte, etc.) in the "Trusted Root" certificate store. If a root certificate is compromised, we must assume all certificates below it to be compromised as well.

A certificate authority (CA) is an entity that issues, or signs, other certificates. To obtain a certificate, an entity (the "subject") will generate a key pair, and send the public key and proof of identity to a CA. The CA will verify the identity of the requester and issue the certificate containing the subject's identity, the public key, and the CA's digital signature. A CA is responsible for saying "yes" these people are whom they claim to be and this is their public key. CAs are authenticated by other CAs or by a root certificate.

An attacker can subvert this process. This can happen when an attacker steals the private key of a CA or of a party to whom a certificate was issued. It can also happen when an attacker impersonates another party when requesting a certificate. In either case, this can result in the issuance of untrustworthy certificates. An attacker might also steal a subject's private key. In such cases, these certificates must be revoked by the issuing authority.

Web of Trust

Another of the three common uses of digital certificates is in the web of trust. This is a less formal method of authentication than PKI provides, but is still in common use. The largest use of the web of trust model is in Pretty Good Privacy (PGP) used for email security. This model is very similar to PKI in that a trusted third party is verifying the authenticity of a certificate. The difference is that this trusted third party is not a CA, but rather a person who endorses the authenticity of another person. Signing the public key of the person requiring endorsement (or trust) with the endorser's (trusted entity) own private key establishes a web of trust. *Figure E.5* illustrates a simple example of a web of trust. If Alice trusts Bob, and Bob trusts Charlie, then Alice implicitly trusts Charlie.

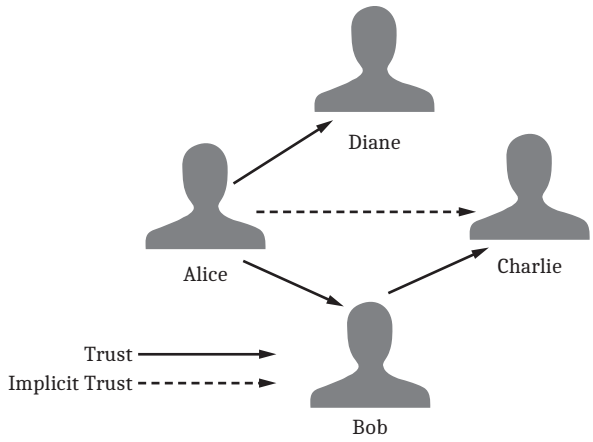


Figure E.5 Web of Trust

Simple Public-Key Infrastructure

The third common use of digital certificates is in the simple public-key infrastructure (SPKI). This model evolved from the need to limit the complexity inherent in public-key infrastructure (PKI) and the associated web of trust. There is no trusted third party in SPKI because the owner and issuer of the certificate are the same entity. For SPKI to be secure, certificates must be preshared among all entities who communicate on that system. This ensures that all knowledge for security decisions resides locally.

Online Certificate Status Protocol (OCSP)

In consideration of the case where an authentic certificate has been stolen, there are methods to revoke certificates. One method is the certificate revocation list (CRL). The CRL method has a few problems that allow a revoked certificate to still be used. This arises from the lag associated with producing CRLs. Also, a certificate will be accepted by default, even if revoked, if the CRL is not accessible.

The online certificate status protocol (OCSP) was created to fix some of these problems. OCSP requires less bandwidth than CRLs and enables near-real-time status checks to verify a certificate's status. OCSP also allows a certificate to be denied by default if the OCSP server is not accessible.

OCSP is a request/response protocol that provides real-time revocation status information for X.509 certificates. When an OCSP-enabled certificate is presented to an application, such as a web browser, the browser uses OCSP to check the certificate and ensure it is valid before proceeding with the session. OCSP uses the following response indicators to help determine certificate revocation status:

- Good: Indicates that the certificate is valid and has not been revoked
- Revoked: Indicates that the certificate has been revoked
- Unknown: Indicates that the responder does not know about the certificate being requested

The system performs a real-time revocation check for each certificate so that if a certificate is compromised or for some other reason requires revocation, it will no longer appear as valid.

Sample X.509 Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,

OU=Certification Services Division,

CN=Thawte Server CA/Email=server-certs@thawte.com

Validity

Not Before: Aug 1 00:00:00 1996 GMT

Not After: Dec 31 23:59:59 2020 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,

OU=Certification Services Division,

CN=Thawte Server CA/Email=server-certs@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:

68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:

85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:

6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:

6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:

```
            29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
            6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
            5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
            3a:c2:b5:66:22:12:d6:87:0d
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
Signature Algorithm: md5WithRSAEncryption
    07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
    a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
    3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
    4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
    8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
    e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
    b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
    70:47
```

This page intentionally left blank

APPENDIX F

Configuring Windows Network Parameters

The SEL-FLR supports network connections using either Dynamic Host Configuration Protocol (DHCP) or a static IP address.

Using DHCP Configuration

The following steps show how to set a computer's network connection for automatic configuration through DHCP.

Step 1. Open the Network Connections Control Panel by typing **ncpa.cpl** in the Windows **Run** dialog box, as shown in *Figure F.1*. Click **OK** to open the Network Connections window, which contains a list of the network devices available on the computer.

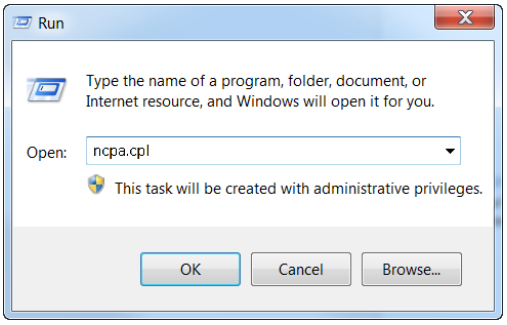


Figure F.1 Open Network Connections With Run Command

Step 2. Right-click the connection you will be using to communicate with the device and click **Properties** to display the Connection Properties window (see *Figure F.2*). For example, if you are connecting via LAN, right-click **Local Area Connection**, as shown in *Figure F.2*.

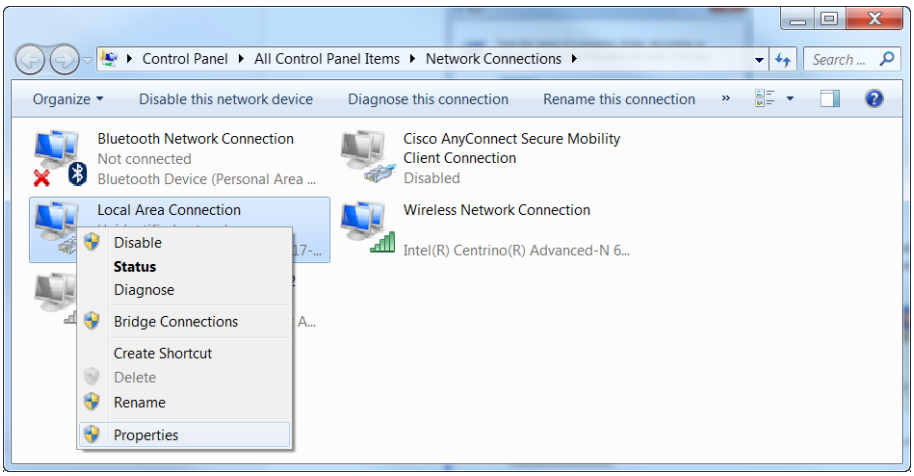


Figure F.2 Open Connection Properties

Step 3. Select **Internet Protocol Version 4 (TCP/IPv4)**, as shown in *Figure F.3*, and click **Properties**.

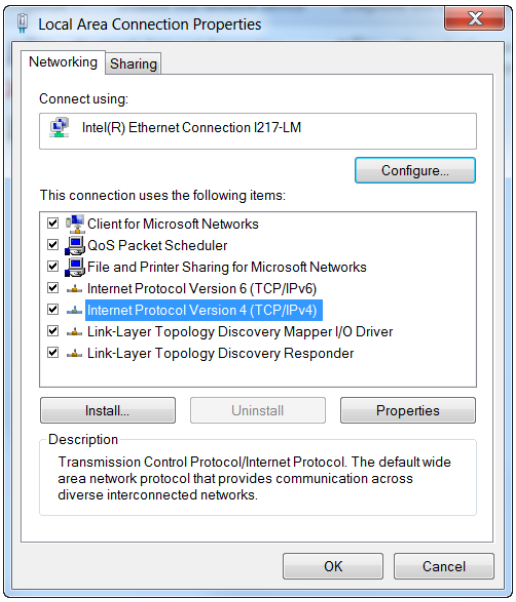


Figure F.3 Local Area Connection Properties

Step 4. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options, as shown in *Figure F.4*. These are typical settings for computers on a company network.

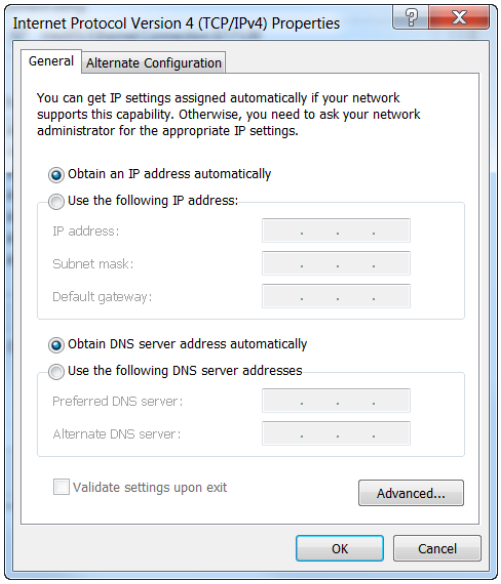


Figure F.4 TCP/IPv4 Properties—DHCP Configuration

Step 5. Click **OK**.

Using Static IP Configuration

The following steps show how to connect to the SEL-FLR by setting a computer's network configuration to a static IP address.

Step 1. Open the Network Connections Control Panel by typing **ncpa.cpl** in the Windows **Run** dialog box, as shown in *Figure F.5*. Click **OK** to open the Network Connections window, which lists the network devices available on the computer.

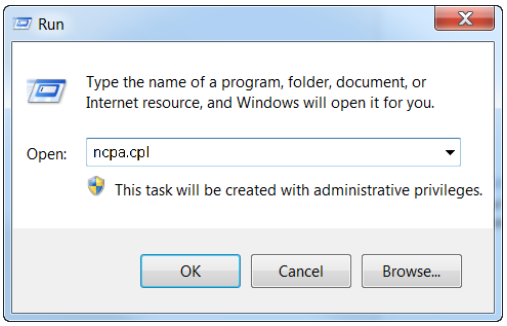


Figure F.5 Open Network Connections With Run Command

Step 2. Right-click the connection you will be using to communicate with the device and click **Properties** to display the Connection Properties window (see *Figure F.6*). For example, if you are connecting via LAN, right-click **Local Area Connection**, as shown in *Figure F.6*.

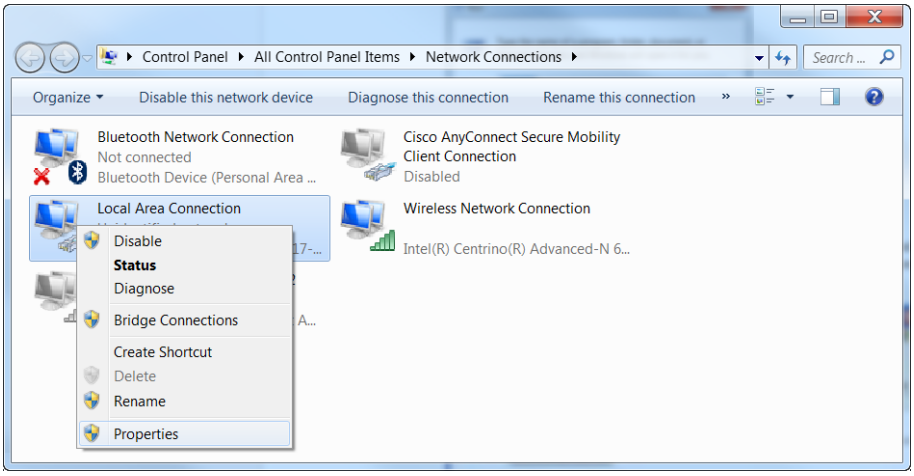


Figure F.6 Open Connection Properties

Step 3. Select **Internet Protocol Version 4 (TCP/IP)**, as shown in *Figure F.7*, and click **Properties**.

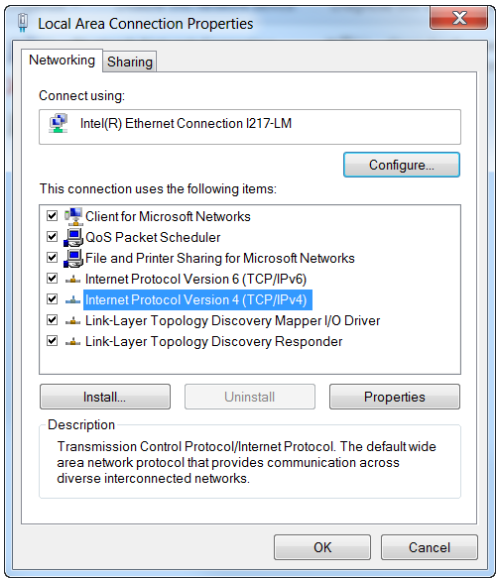


Figure F.7 Local Area Connection Properties

Step 4. Select **Use the Following IP Address** and choose an IP address and subnet for the computer, as shown in *Figure F.8*. The subnet determines the valid range of IP addresses. By default, the **Subnet mask** field is set to 255.255.255.0. This means that the first three sets of numbers in the IP address must be the same for both the SEL-FLR and your computer.

By default, the IP address of the **ETH F** port is 192.168.1.2. If you leave the subnet mask at its default value, your computer can connect by using any IP address in the 192.168.1.*xxx* range, where *xxx* is either 1 or a number from 3 to 254.

You do not have to choose a gateway. Although the Domain Name System (DNS) is set to manual configuration, you do not need to enter a configuration.

NOTE: If you configure your computer to use a static IP address, you will need to enter the IP address of the SEL-FLR management interface into your browser to access the SEL-FLR.

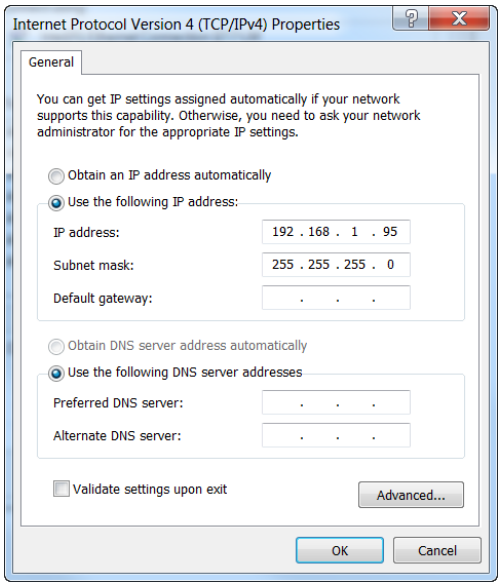


Figure F.8 TCP/IPv4 Properties—Manual Configuration

Step 5. Click **OK**.

APPENDIX G

Acronym List

AES	Advanced Encryption Standard
CA	Certificate Authority
CRSRTT	Current Reset Secondary Reset Test Tool
EIRP	Effective Isotropic Radiated Power
FCI	Faulted Circuit Indicator
FLR	Fault and Load Receiver
FLT	Fault and Load Transmitter
FSPL	Free-Space Path Loss
LOC	Loss of Current
MAC	Media Access Control (Address)
MOT	Model Option Table
MSDS	Material Safety Data Sheet
RAM	Random-Access Memory
RF	Radio Frequency
RNG	Random Number Generator
RSSI	Received Signal Strength Indicator
SPKI	Simple Public-Key Infrastructure
TLS	Transport Layer Security

This page intentionally left blank

APPENDIX H

SEL-FLR Enclosure

Introduction

The SEL-FLR enclosure provides a flexible, off-the-shelf solution for deploying the SEL-FLR at multiple locations throughout a power system. The SEL-FLR enclosure includes a power supply and battery backup, and can come prewired with an SEL-3061 for cellular backhaul. The enclosure can also be ordered with space and available power for users to connect their own third-party radio for wireless backhaul from the SEL-FLR to SCADA. The enclosure also has space and available power to allow users the option of installing an SEL-3505 for additional edge intelligence and automation. *Figure H.1* provides a high-level overview of the components and layout of the enclosure.

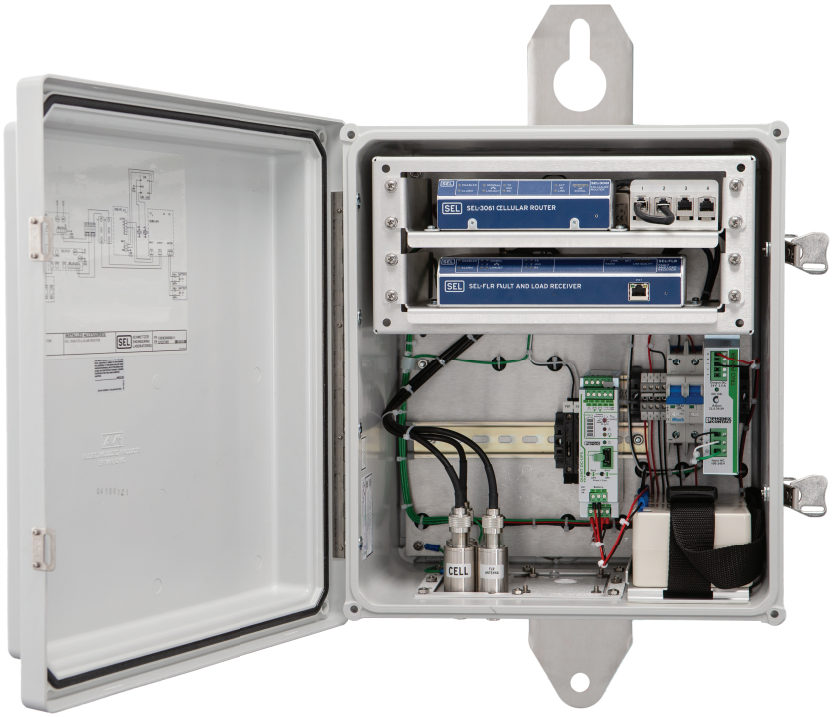


Figure H.1 SEL-FLR Enclosure Layout

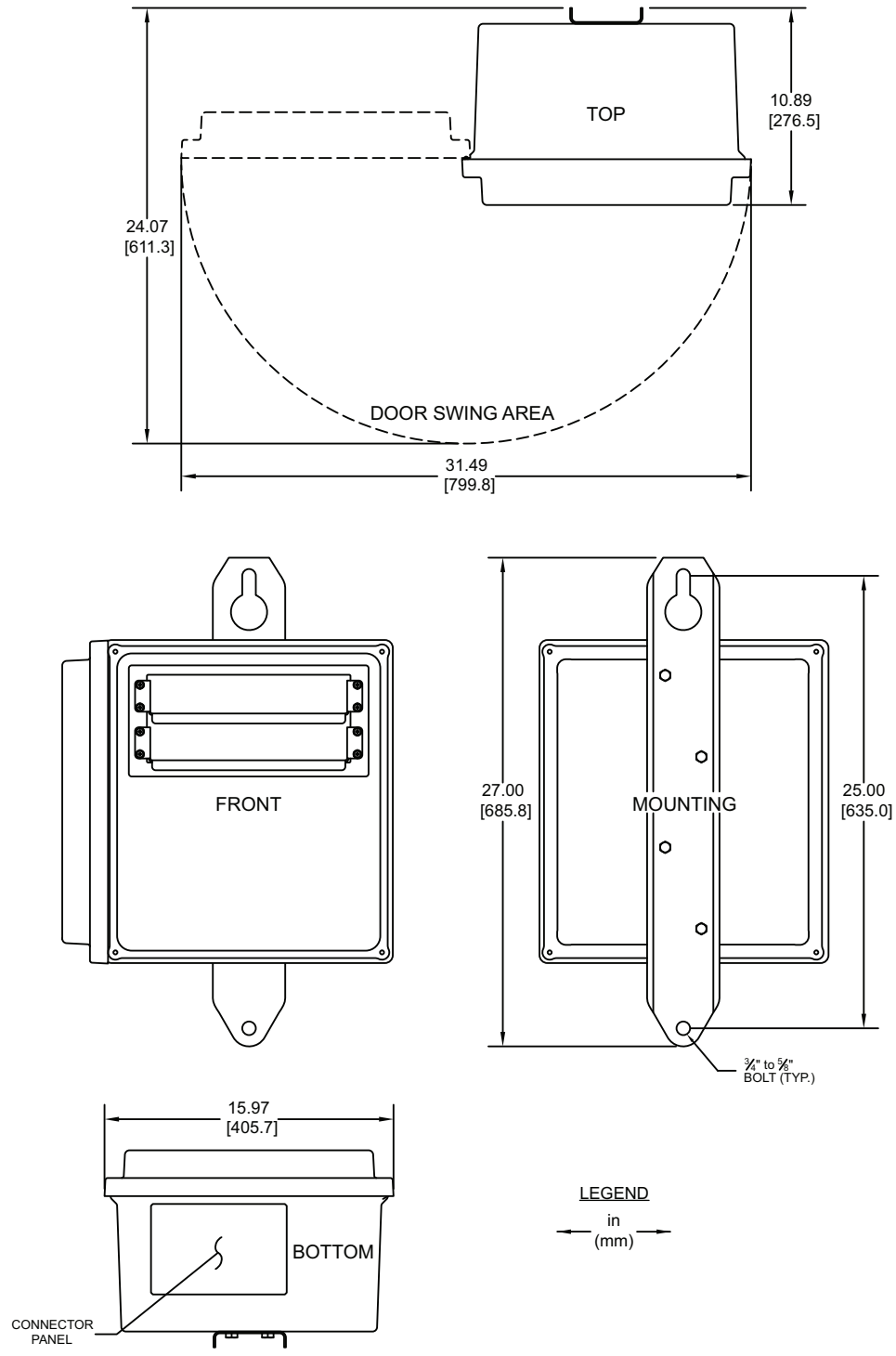


Figure H.2 SEL-FLR Enclosure Dimensions

Installation

The SEL-FLR enclosure is ideal for pole-mounted applications. SEL does not supply the hardware assemblies required for mounting the enclosure. The SEL-FLR enclosure requires external 120 Vac power. SEL recommends that the

control power transformer serving the enclosure be on the same pole as the enclosure, and that any user-supplied radio, RTAC, or other equipment is installed prior to mounting the enclosure in the field. *Figure H.3* shows a detailed view of the drillable connector plate on the bottom of the enclosure. All field connections should be made through the connector plate. This plate includes three surge suppressors with N-type connectors for connection of SEL-FLR and backhaul radio antenna cables.

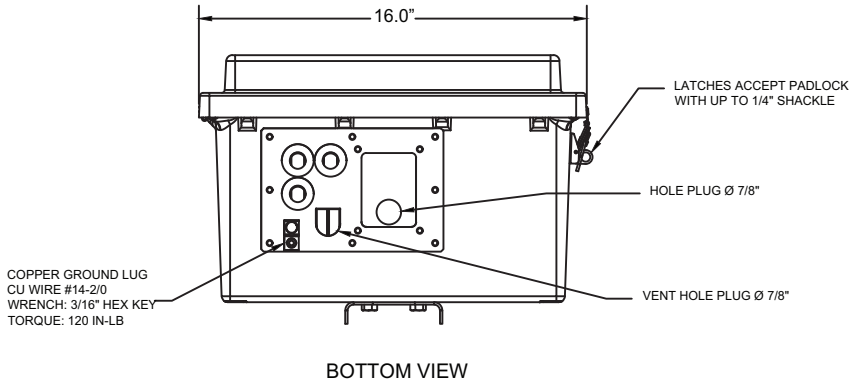


Figure H.3 SEL-FLR Enclosure Connector Plate

Communication Port Connections

When supplied with an installed SEL-3061, the communication connections in the enclosure come prewired. An Ethernet patch panel inside the enclosure provides easy access to rear ports of the SEL-FLR and SEL-3061 without the need to remove installation shelves. *Figure H.4* details communication port connections prewired in the factory.

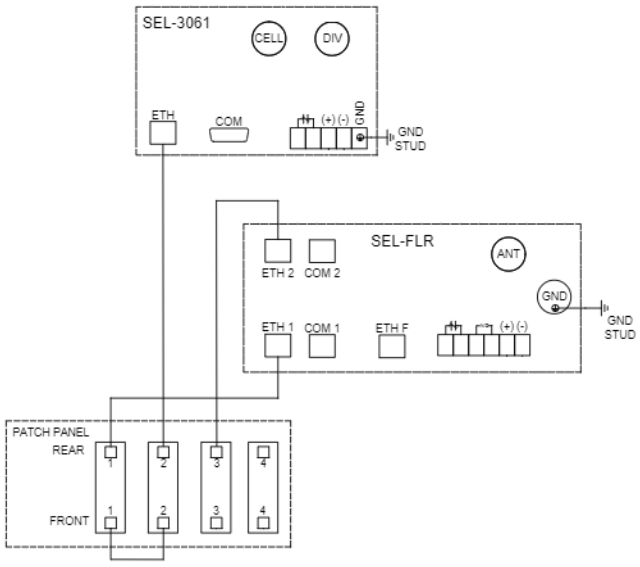


Figure H.4 Communication Port Connection Diagram

This page intentionally left blank

Glossary

Active Threshold	The lowest trip setting at which the SEL-FLT will detect a fault condition.
Arming Requirement	A condition that must be met before the SEL-FLT can detect events.
AutoRANGE	Logic that automatically adjusts the trip threshold based on measured load current.
CRSRTT	A magnet tool used to interface with the SEL-FLT.
Delay Trip	Minimum duration for which current must remain above the trip threshold before the SEL-FLT registers a fault and trips.
Device Reset	Hardware power cycle.
Discovered	Radio state of an unjoined SEL-FLT device that has been found by one or more SEL-FLR devices, but which has not yet joined a network.
Discovery List	The SEL-FLR list of SEL-FLT devices that are within range of the SEL-FLR and are broadcasting an Unjoined Radio status.
Disturbance	A fault event (current spike) detected by the SEL-FLT, but not the system protection (i.e., no outage).
Fault Stimulus	An event in which the system current exceeds the SEL-FLT trip threshold.
Faulted Circuit Indicator (FCI)	A line-mounted device used to detect and report short-circuit fault conditions.
Inrush Restraint	A feature designed to prevent device tripping from current inrush during system energization (e.g., automated reclosing or system restoration).
Joined	Radio status meaning that the SEL-FLT and SEL-FLR have established secure communication and data are being exchanged.
Joining	Radio status meaning that the SEL-FLT and SEL-FLR are actively exchanging key/authentication information.
Local Display	Visual LED indication used to show the state of the device and indicate events (faults or outages).
Loss of Current	An event in which the system current drops below the minimum current threshold.
Lost Link	Radio status meaning that the SEL-FLT and SEL-FLR communication has been interrupted for some reason, and data are no longer being exchanged.
Momentary Fault	An event in which the system current exceeds the SEL-FLT trip threshold followed by a successful reclose.
Momentary Loss of Current	An event in which the system current drops below the minimum current threshold followed by a successful reclose.
Permanent Fault	An event in which the system current exceeds the SEL-FLT trip threshold followed by an outage (i.e., unsuccessful reclose/lockout).

Permanent Loss of Current An event in which the system current drops below the minimum current threshold followed by an outage (i.e., unsuccessful reclose).

Radio Network Refers to all of the SEL-FLT devices joined to a single SEL-FLR receiver.

Rejoining Radio status meaning that an SEL-FLT and SEL-FLR are actively trying to re-establish communication, and are re-exchanging key/authentication information.

Trip An FCI device behavior after detecting a fault.

Trip Current The actual fault current value in rms necessary in order for the SEL-FLT to detect a fault.

Trip Threshold The nominal current rating necessary for the SEL-FLT to detect a fault.

Undiscovered Radio state of an unjoined SEL-FLT that has not been found by any SEL-FLR Receivers.

Unlinked Radio status meaning that the SEL-FLT and SEL-FLR are not communicating with each other. This status can have two states: Discovered and Undiscovered.

Whitelist The list of SEL-FLT devices that are allowed to join with a particular SEL-FLR. The whitelist is stored and managed in the SEL-FLR.