Preliminary Copy

SEL-3022

Wireless Encrypting Transceiver

Instruction Manual

20050615

Attention

The SEL-3022 is a cryptographic device. Limit access to the SEL-3022, SEL-5809 Settings Software, SEL-5810 Virtual Serial Software, and SEL-3022 Instruction Manual to authorized personnel only. Do not copy these items. Securely store these items when not in use. Destroy these items when no longer needed.

SCHWEITZER ENGINEERING LABORATORIES

Making Electric Power Safer, More Reliable, and More Economical®

Preliminary Copy

CAUTION: Removal of enclosure panels exposes circuitry which may cause electrical shock which can result in injury.

ATTENTION: Le retrait des panneaux du boîtier expose le circuit qui peut causer des chocos électriques pouvant entraîner des blessures.

The software (firmware), drawings, commands, and messages are copyright protected by the United States Copyright Law and International Treaty provisions. All rights are reserved.

You may not copy, alter, disassemble, or reverse-engineer the software. You may not provide the software to any third party.

All brand or product names appearing in this document are the trademark or registered trademark of their respective holders.

ACSELERATOR, Connectorized, Job Done, MIRRORED BITS, Schweitzer Engineering Laboratories, SEL, SEL, SELOGIC, SEL-PROFILE, and CONSELTANT are registered trademarks of Schweitzer Engineering Laboratories, Inc.

The English language manual is the only approved SEL manual.

© 2005 Schweitzer Engineering Laboratories. All rights reserved.

This product is covered by U.S. Patent(s) Pending, and Foreign Patent(s) Issued and Pending.

This product is covered by the standard SEL 10-year warranty. For warranty details, visit www.selinc.com or contact your customer service representative.

PM3022-01

Preliminary Copy

Table of Contents

List of Tables iii

List of Figures v

Preface vii

Section 1: Introduction & Specifications

Introduction 1.1
Product Overview 1.2
Application Overview 1.5
Connections, Reset Button, and LED Indications 1.6
Software System Requirements 1.10
General Safety and Care Information 1.11
Specifications 1.12

Section 2: Installation

Introduction 2.1
Dimension Drawing 2.2
Setting Up Your PC or PDA With the SEL-5809 and SEL-5810 Software 2.3
Initializing the SEL-3022 ..... 2.7

Section 3: Job Done Example

Introduction 3.1
Job Done Example 1 ..... 3.2

Section 4: Settings and Commands

Introduction 4.1
Serial Port Settings 4.2
Wireless Port Settings 4.3
Communication Status Command 4.6
Device Information 4.7

Section 5: Testing and Troubleshooting

Introduction 5.1
Testing Philosophy 5.2
Communications Channel Diagnostics 5.4
Self-Tests 5.6
Troubleshooting 5.7
Factory Assistance 5.8

Preliminary Copy

Appendix A: Firmware and Manual Versions

Firmware A.1
Instruction Manual A.2

Appendix B: Firmware Upgrade Instructions

Introduction B.1
Factory Assistance B.8

Appendix C: Wireless Operator Interface Security

Introduction C.1
Wireless Interface Security Overview C.2
IEEE 802.11 WEP Security C.5
The SEL Security Application C.9

Appendix D: Certificates

Glossary GL.1

Preliminary Copy

List of Tables

Table 1.1 DCE (Female DB9) 1.8
Table 1.2 Operating Systems and Wireless Modules Tested With the SEL-5809 Settings Software 1.10
Table 4.1 Settings: DCE Port 4.2
Table 4.2 Settings: Wireless 4.3
Table 4.3 Settings: WEP Keys 4.4
Table 4.4 Settings: User 4.4
Table 4.5 Settings: Operator 4.5
Table 4.6 Settings: Security Officer 4.5
Table 4.7 Status Command Names and Descriptions 4.6
Table 4.8 Identification 4.7
Table 4.9 Status: Device 4.7
Table 4.10 Status: Output Alarm 4.8
Table 4.11 Status: Virtual Serial Port 4.8
Table 5.1 Status: Comm 5.4
Table 5.2 Device Status: Device Status 5.4
Table 5.3 SEL-3022 Self-Test Capabilities 5.6
Table 5.4 Troubleshooting 5.7
Table A.1 Firmware Revision History A.1
Table A.2 Instruction Manual Revision History A.2
Table C.1 Number of Years Required to Guess an SEL-3022 Password C.13

Preliminary Copy

This page intentionally left blank

Preliminary Copy

List of Figures

Figure 1.1 Typical SEL-3022 and SEL-5810 Virtual Serial Software Application 1.2
Figure 1.2 Encrypted Packet Stream 1.4
Figure 1.3 Typical Connections for the SEL-3022 ..... 1.6
Figure 1.4 Typical Alarm Output Installation 1.8
Figure 2.1 SEL-3022 Dimension Drawing 2.2
Figure 2.2 Windows Run Command 2.3
Figure 2.3 Product Unregistered Prompt 2.4
Figure 2.4 Select a Device Type to Create 2.7
Figure 2.5 Specify New Device Location 2.8
Figure 2.6 Opening Device 2.8
Figure 2.7 Identification Screen 2.9
Figure 2.8 Status: Device 2.10
Figure 2.9 Settings: Wireless 2.10
Figure 2.10 Settings: WEP Keys 2.11
Figure 2.11 Settings: User 2.11
Figure 2.12 Settings: Operator 2.12
Figure 2.13 Settings: Security Officer 2.12
Figure 2.14 Confirm Send Prompt 2.13
Figure 2.15 Send Operation Message 2.13
Figure 2.16 Select Items to Print 2.14
Figure 2.17 Print Window 2.14
Figure 3.1 Remotely Located Recloser Control 3.2
Figure 3.2 Job Done Example SEL-5809 Top Level View 3.3
Figure 3.3 Select a Wireless Session for DNP3 Job Done Example 3.4
Figure 3.4 Settings: DCE Port 3.4
Figure 3.5 Status: Virtual Serial Port With Connection Status Red 3.5
Figure 3.6 Communication Parameters Window in ACSELERATOR 3.6
Figure 3.7 Status: Virtual Serial Port With Connection Status Green 3.6
Figure 3.8 Reading Settings Via the SEL-3022 ..... 3.7
Figure 3.9 Monitoring SEL-651R Meter Data Via the SEL-3022 ..... 3.8
Figure 3.10 Status: Virtual Serial Port Connection Status Red 3.9
Figure 3.11 Specify Device to Export to SEL-5810 Virtual Serial Software 3.10
Figure 3.12 Export Encrypted User Configuration File 3.10
Figure 3.13 Store Encrypted File 3.11
Figure 3.14 Password Prompt in SEL-5810 Virtual Serial Software 3.12
Figure 3.15 Communication Parameters Window in ACSELERATOR 3.13
Figure 3.16 Reading SER Report Via ACSELERATOR 3.14
Figure B.1 PC to SEL-3022 Connection B.2
Figure B.2 SEL-3022 and SEL-5809 Connection Parameters B.2

Preliminary Copy

Figure B.3 SEL-5809 Settings Software Connection Method B.3
Figure B.4 SEL-5809 Opening Connection B.3
Figure B.5 Status: Device Window B.4
Figure B.6 Confirmation Prompt..... B.4
Figure B.7 Send Operation Prompt B.4
Figure B.8 Configuring Serial Port Settings in the Terminal Software..... B.5
Figure B.9 Send File Prompt..... B.6
Figure B.10 Sending Confirmation Window..... B.6
Figure B.11 Terminal Invalid Firmware Error Message B.7
Figure B.12 Terminal Valid Firmware Message B.7
Figure C.1 Two Independent Layers of Cryptographic Security Protect the SEL-3022 Wireless Operator Interface C.2
Figure C.2 Operation of the HMAC SHA-1 Keyed Hash Authentication Function C.9
Figure C.3 Operation of the AES Encryption Function C.10
Figure C.4 SEL-3022 Security Application Overview C.11
Figure C.5 Wireless Interface Session Authentication Dialog C.15

Preliminary Copy

Preface

Manual Overview

The SEL-3022 Wireless Encrypting Transceiver Instruction Manual describes common aspects of the wireless encrypting transceiver application and use. It includes the necessary information to install, set, test, and operate the transceiver.

An overview of each manual section and topics follows:

Preface. Describes the manual organization and conventions used to present information.

Section 1: Introduction & Specifications. Introduces SEL-3022 applications, cabling and external connections, and PC and PDA Software system requirements. This section also lists specifications.

Section 2: Installation. Provides dimension drawings on the SEL-3022 and instructions for setting up your PC or PDA, and initializing the SEL-3022.

Section 3: Job Done Example. Provides a Job Done® example for applying the SEL-3022 to an SEL-651R Recloser Control mounted twenty feet above the street.

Section 4: Settings and Commands. This section lists all the SEL-3022 settings including those for serial port, wireless port, encryption parameters, and SCADA protocol. Includes information on the communication status command for analyzing and monitoring the status of the SEL-3022 serial port communication channel.

Section 5: Testing and Troubleshooting. Describes the SEL-3022 self-test along with troubleshooting guidelines.

Appendix A: Firmware and Manual Versions. Lists firmware and manual revision dates and description of modifications.

Appendix B: Firmware Upgrade Instructions. Describes the procedure to update the firmware stored in flash memory.

Appendix C: Wireless Operator Interface Security. Discusses how the SEL-3022 incorporates a wireless LAN interface including recommended security settings. Explains the additional AES encryption and cryptographic authentication employed on the wireless operator interface.

Appendix D: Certificates. Describes certificates related to the SEL-3022.

Page Numbering

This manual shows page identifiers at the top of each page; see the figure below.

Page Number Format

The page number appears at the outside edge of each page; a vertical bar separates the page number from the page title block. The page numbers of the SEL-3022 Serial Encrypting Transceiver Instruction Manual are represented by the following building blocks:

- Section number
- Actual page number in the particular section

The section title is at the top of the page title block, with the main subsection reference in bold type underneath the section title.

Cross-References

Cross-references are formatted as described below in both the hard copy and electronic documentation for the SEL-3022. In the electronic documentation, clicking with the mouse on cross-references takes you to the referenced location.

- References to figures, tables, examples, and equations include only the referenced item:
  - *Table 3.1* (*3* indicates the section number)
  - *Figure 4.5* (*4* indicates the section number)
- References to headings on another page include the heading title and the page number:
  - *Disconnect Monitoring on page 3.8*

Examples

This instruction manual uses several example illustrations and instructions to explain how to effectively operate the SEL-3022. These examples are for demonstration purposes only; the firmware identification information or settings values included in these examples may not necessarily match those in the current version of your SEL-3022.

Safety Information

This manual uses hazard statements, formatted and defined as follows:

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

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

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

Preliminary Copy

This page intentionally left blank

Preliminary Copy

Section 1

Introduction & Specifications

Introduction

This section includes the following overviews of the SEL-3022 Wireless Encrypting Transceiver:

- Product Overview
- Application Overview
- Connections, Reset Button, and LED Indications
- Software System Requirements
- General Safety and Care Information
- Specifications

Cryptographic Manual—Do Not Copy
Preliminary Copy

Product Overview

The SEL-3022 Wireless Encrypting Transceiver is an EIA-232 to IEEE 802.11b, or WiFi, encryption device that adds strong encryption and authentication features to the data sent across wireless ports. The companion SEL-5809 Settings Software and SEL-5810 Virtual Serial Software programs allow legacy Personal Computer (PC) programs, such as HyperTerminal®, Relay Gold®, or ACSELERATOR® SEL-5030 Software, that use EIA-232 serial ports to securely communicate with the SEL-3022 via PC or Personal Digital Assistant (PDA) wireless (IEEE 802.11b) ports. See *Figure 1.1*.

The SEL-3022, with the SEL-5809 Settings Software and SEL-5810 Virtual Serial Software securely transmits and receives data between Intelligent Electronic Devices (IEDs) and PCs (or PDAs) via an IEEE 802.11b wireless connection. The SEL-3022 and SEL-5810 Virtual Serial Software provide a retrofit solution that allows you to continue to use standard PC programs while providing encrypted and authenticated wireless connectivity with IEDs. See *Figure 1.1*.

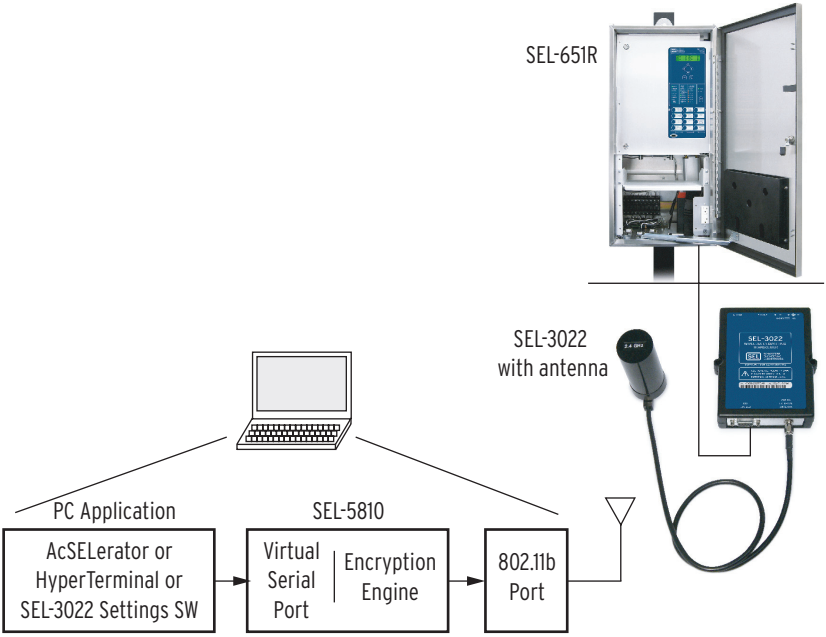

Figure 1.1 Typical SEL-3022 and SEL-5810 Virtual Serial Software Application

SEL-3022 Transceiver

The SEL-3022 consists of two communication ports: the EIA-232 and IEEE 802.11b. The EIA-232 serial port connects to an IEDs EIA-232 serial port. The SEL-3022 and IED exchange unencrypted data such as engineering access data. The SEL-3022 forms an authentication message and encrypts the data received by the IED then passes it to the IEEE 802.11b port. The IEEE 802.11b communication port transmits the encrypted data to the PC/PDA running the SEL-5809 Settings Software or SEL-5810 Virtual Serial Software. When the SEL-3022 802.11b port receives a message it decrypts and authenticates the message. If the message decrypts and authenticates correctly the message is passed to the serial port, otherwise the session is terminated.

SEL-5809 Settings Software and SEL-5810 Virtual Serial Software

The SEL-5809 Settings Software and SEL-5810 Virtual Serial Software are used to communicate with the SEL-3022. The SEL-5809 Settings Software consists of three major functions or roles: Security Officer, Operator, and User. The security officer has access to all of the SEL-3022 configuration parameters including the cryptographic settings. The operator has access to all of the SEL-3022 configuration parameters except the cryptographic settings. Both the security officer and operator modes are used to configure the SEL-3022. The user role generates a virtual serial port that allows applications to encrypt and decrypt data between the PC and the IED that the SEL-3022 is connected to. In the user role you cannot modify SEL-3022 configuration parameters. To change roles you must exit the current role and reestablish a connection to the new access level.

The SEL-5810 Virtual Serial Software is a subset of the SEL-5809 Settings Software, and only allows connection to the SEL-3022 in the user role.

Your company security officer, or person in charge of configuring cryptographic settings, would typically use the SEL-5809 Settings Software to configure the SEL-3022 transceivers. After the SEL-3022 transceivers have been configured the security officer can configure a PC and PDA with the SEL-5810 Virtual Serial Software for field personnel (i.e., workers who need engineering access to the IEDs connected to the SEL-3022 transceivers, but who do not need to configure the SEL-3022 transceivers).

Both the SEL-5809 Settings Software and SEL-5810 Virtual Serial Software allow you to integrate your standard EIA-232 serial port programs with wireless port via the SEL-5810 Virtual Serial Software encrypting engine to a 802.11b port. When the SEL-5809 Settings Software/SEL-5810 Virtual Serial Software receives a message from a PC program, ACSELERATOR for example, the virtual serial port generates an authentication message that is appended to the original message, which is then encrypted. The SEL-5809 Settings Software/SEL-5810 Virtual Serial Software then passes the encrypted message to the 802.11b port for transmission to the SEL-3022.

When the SEL-5809 Settings Software/SEL-5810 Virtual Serial Software receives a message from the wireless port, it decrypts and authenticates the message and passes it to the virtual serial port which in turn passes it to your PC program. See *Figure 1.2*.

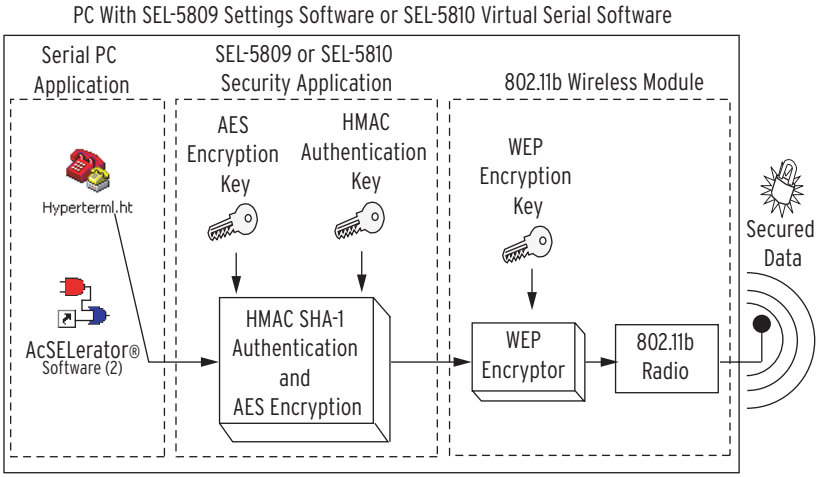

Figure 1.2 Encrypted Packet Stream

Application Overview

The SEL-3022 is ideal for applications where engineering access communication is required but the IED is installed in a location where physical access is limited. For example, often recloser controls are mounted in inconvenient locations either because of power line location or to keep them out of reach of unauthorized users. In either case, for an engineer or lineman to communicate with the recloser control, he must traverse these obstacles to gain physical access to the IED. This includes opening the recloser control cabinet, which will expose the inside of the control to the weather.

Through use of the SEL-3022, the lineman simply drives within distance of the recloser control, establishes a wireless communication link using the SEL-5810 Virtual Serial Software, and then retrieves the fault location data or modifies settings—all from the comfort and safety of his vehicle. Further, because this communication link does not require the lineman to open the recloser control, the internal electronic panel is not exposed to rain, snow, or dust.

Cryptographic Manual—Do Not Copy
Preliminary Copy

Connections, Reset Button, and LED Indications

The figure below shows typical connections for the SEL-3022.

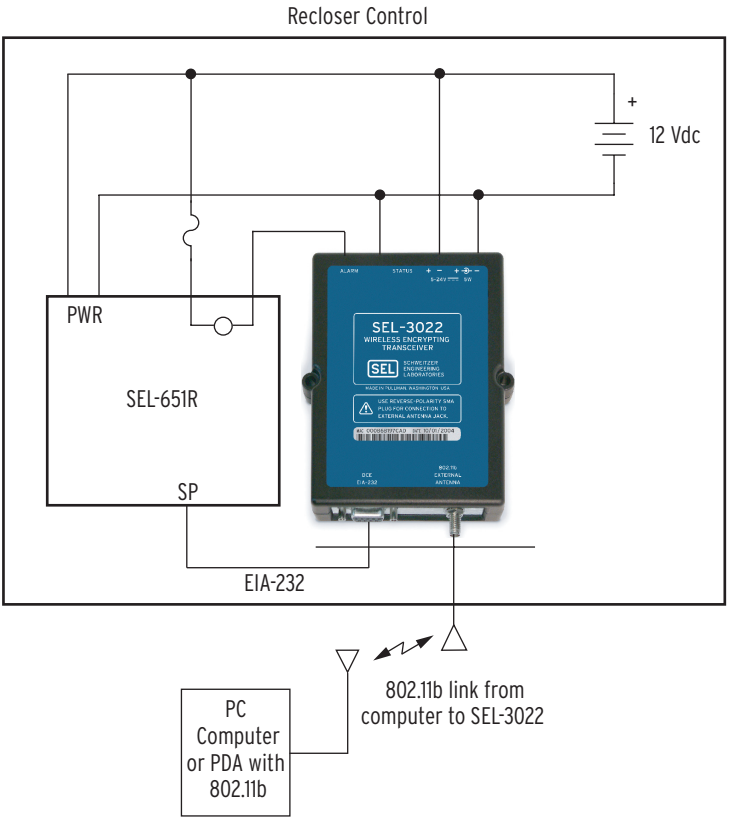

Figure 1.3 Typical Connections for the SEL-3022

Power Supply Connections

You can apply 5 to 24 Vdc directly to the SEL-3022 power terminals, which are available either as compression terminals or a 2.5 mm jack. If the power source voltage is not within the 5 to 24 Vdc range, use an auxiliary power supply to provide 5 to 24 Vdc to the SEL-3022. See *Specifications on page 1.12* for power requirements.

Preliminary Copy

IMPORTANT: Do NOT wire power to both the compression terminals and the 2.5 mm jack. Use only one power connection at a time.

Alarm Output Connection

Use the solid-state alarm contact to alert you to problems either with the communications channel or the SEL-3022. See *Section 5: Testing and Troubleshooting* for more details. To maintain the UL rating of the SEL-3022, connect the alarm output contact as follows:

1. Use an external load to limit current to less than 100 mA through the alarm contact. There is no means within the SEL-3022 to limit current through the alarm contact. You must ensure that the external circuit connected to the SEL-3022 limits the current. For example, a typical SEL contact input draws 4 mA. *Figure 1.4* shows a typical connection of a wetting source (125 Vdc), the SEL-3022 solid-state output, an SEL-2030 contact input, and an optional load resistor. In this case, because the contact input impedance limits the current to less than 100 mA, the load resistor is not necessary. If the sensing input does not have a means of limiting the current to less than 100 mA, then you must use a high wattage resistor. Select a load resistor with the proper wattage rating to limit the current. For example, assume the wetting source is 125 Vdc and that the sensing input requires 10 mA to assert. You can use the following calculation to determine the load resistor: 125 Vdc/ 10 mA = 12.5 kΩ. Calculate the minimum wattage: $(10\ \text{mA})^2 \bullet 12.5\ \text{k}\Omega = 1.25\ \text{W}$. You would typically double this parameter to 2.5 W to ensure proper operation over temperature and life. You should verify proper derating with the resistor data sheet.
2. Circuit protection should include an in-line fuse rated for 0.5 A or less with a voltage rating greater than the voltage you intend to use.

Figure 1.4 shows a typical alarm output installation.

CAUTION: Current through the alarm output must be limited to less than 100 mA.

Preliminary Copy

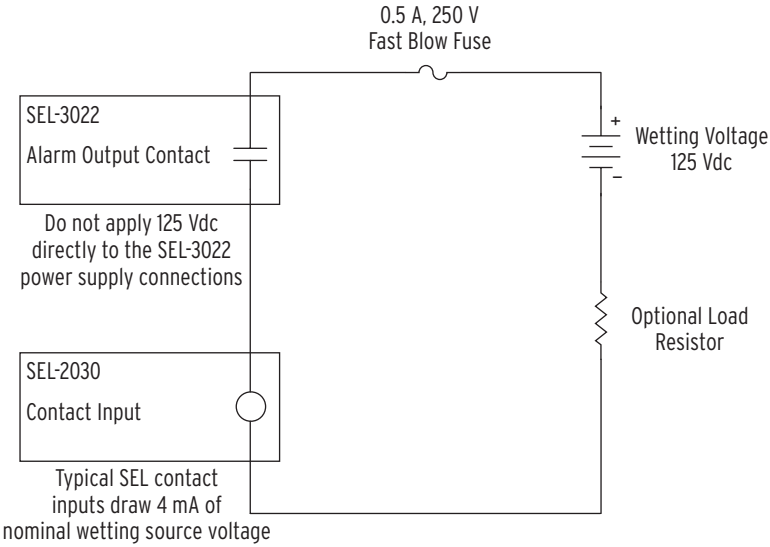

Figure 1.4 Typical Alarm Output Installation

Serial Port Pin-Out Connection

The SEL-3022 has a fully compliant DCE serial port. SEL offers many cable configurations for use between the SEL-3022 and other devices.

The serial port pin-out descriptions for the DCE port are as follows.

Table 1.1 DCE (Female DB9)

Pin	Description
1	Data Carrier Detect (Output)
2	Transmitted Data (Output)
3	Received Data (Input)
4	Data Terminal Ready (Input)
5	Ground
6	Data Set Ready (Output)
7	Request to Send (Input)
8	Clear to Send (Output)
9	Ring Indicator (Output)

Preliminary Copy

Reset Button

Use the {RESET} button to reset and delete all security related settings. You can access the {RESET} button through the small hole in the end of the SEL-3022 near the status LED. Use a paper clip or other similar device to press the {RESET} button for at least 2 seconds, which resets the SEL-3022 into a default state. Power must be applied to the SEL-3022 for the reset operation to occur.

IMPORTANT: Pressing the {RESET} button erases all security parameters and interrupts transmission of encrypted data until you initialize the SEL-3022. See Initializing the SEL-3022 on page 2.7 in Section 2: Installation.

Status LED

Use the status LED to determine the state of the SEL-3022. If the status LED is solidly illuminated, the SEL-3022 is operating correctly. If the LED is blinking, the SEL-3022 is in a failed or reset mode. Refer to *Section 5: Testing and Troubleshooting* for more details.

Software System Requirements

The SEL-3022 comes with configuration and monitoring software, referred to as the SEL-5809 Settings Software and the SEL-5810 Virtual Serial Software. The SEL-5809 Settings Software is the only means to set and monitor the SEL-3022. The software comes in two versions: one version is for a PC and one is for a PDA operating system. The following operating systems have been tested with the software.

Table 1.2 Operating Systems and Wireless Modules Tested With the SEL-5809 Settings Software

Devices	Qualified Systems
PCs	Windows® XP Professional Edition (Service Pack 1) Windows 2000 (Service Pack 4) with .NET framework (Version 1.1) installed Windows XP with .NET framework installed
PDAs	Pocket PC 2002/2003 or higher with .NET compact framework (Version 1.0 Service Pack 3)
Wireless (802.11b) Modules	Netgear MA111 Linksys WPC11

Preliminary Copy

General Safety and Care Information

General Safety Notes

The SEL-3022 is designed for restricted access locations. Access shall be limited to qualified service personnel.

The SEL-3022 should not be installed or operated in a condition not specified in this manual.

CAUTION: The SEL-3022 is an intentional radiator. Changes or modifications not expressly approved by SEL for compliance could void the user's authority to operate the equipment.

CAUTION: The SEL-3022 is an intentional radiator. The radio has been authorized by the FCC for mobile use only. Users and nearby persons must maintain a separation distance of at least 20 cm (8 inches) from the radio during operation.

Cleaning Instructions

The SEL-3022 should be de-energized (by removing the power connection to both the power and alarm connection) before cleaning.

The case can be wiped down with a damp cloth. Solvent-based cleaners should not be used on plastic parts or labels.

Preliminary Copy

Specifications

Indicators

Green LED: Device Status

Solid-State Output

100 mA continuous
250 Vdc or 120 Vac Operational Voltage

Max. On Resistance:	50 Ω
Min. Off Resistance:	10 MΩ
Insulation:	1500 Vdc
Wiring size:	14 AWG Max. 26 AWG Min. 0.4 mm Min. Insulation 105°C, 250 V Min.

Encryption Protocols

AES: 128-bit encryption

Serial Port

Connectors:	DB-9 Female (DCE)
Data Rate:	300 bps to 38400 bps
Interface:	EIA-232

WiFi/802.11b Configuration Port

Protocol:	IEEE 802.11b
Modulation:	DSSS
Frequency Band:	2.4 GHz
Encryption:	128-bit WEP and 128-bit AES
Authentication:	HMAC SHA-1 128-bit key
External Antenna:	Reverse Polarity
Connector:	SMA Jack

Power Requirements

+5 to +24 Vdc: <5 W
supplied through compression terminals or a 2.5 mm jack

Operating Temperature Range

–40° to +85°C (–40° to +185°F)
5 to 95% humidity (noncondensing)

Dimensions

3.675" wide
4.8" deep
1" high, without DIN mount

Type Tests

Electromagnetic Compatibility

Radiated Emissions:	IEC 60255-25:2000, Class A FCC part 15 Class A

Electromagnetic Compatibility Immunity

Conducted RF Immunity:	ENV 50141:1993, 10 V rms IEC 61000-4-6:1996, 10 V rms
Digital Radio Telephone RF:	ENV 50204:1995, 10 V/m at 900 MHz and 1.89 GHz
Electrostatic Discharge:	IEC 60255-22-2:1996, IEC 61000-4-2:1999, [EN 61000-4-2-1995], Levels 1, 2, 3, 4
Fast Transient Disturbance:	IEC 61000-4-4:1995, IEC 60255-22-4:1992, 4 kV at 2.5 and 5 kHz
Radiated Radio Frequency:	ENV 50140-1993, IEC 60255-22-3:1989, 10 V/m IEEE C37.90.2-1995, 35 V/m

Type Test Compliance Criteria:

1) The SEL-3022 does not damage or impede IED operation.
2) The SEL-3022 is allowed to lose data during testing events.
3) The SEL-3022 must recover without external intervention.

Environmental

Cold:	IEC 60068-2-1:1990 [EN 60068-2-1-1993], Test Ad: 16 hrs @ –40°C
Dry Heat:	IEC 60068-2-2:1974 [EN 60068-2-2-1993], Test Bd: 16 hrs @ +85°C
Damp Heat, Cyclic:	IEC 60068-2-30:1980, Test Db: +25° to +55°C, 6 cycles, 95% humidity
Vibration:	IEC 60255-21-1:1988, Class 1 IEC 60255-21-2:1988, Class 1 IEC 60255-21-3:1993, Class 2
Max. Altitude:	2000 m

Preliminary Copy

Certifications

ISO:	Device is designed and manufactured using ISO 9001 certified quality program.
Listings:	IEC 60950-1: 1st Ed./ CSA C22.2 No.60950-1/ EN 60950-1
FCC:	15.247
IC:	ICES-001

Preliminary Copy

This page intentionally left blank

Preliminary Copy

Section 2

Installation

Introduction

This section includes the following:

- Dimension Drawing
- Setting Up Your PC or PDA With the SEL-5809 Settings Software and SEL-5810 Virtual Serial Software.
- Initializing the SEL-3022: Discusses the settings required to initialize the SEL-3022 when the SEL-3022 is in a reset condition.

Preliminary Copy

Dimension Drawing

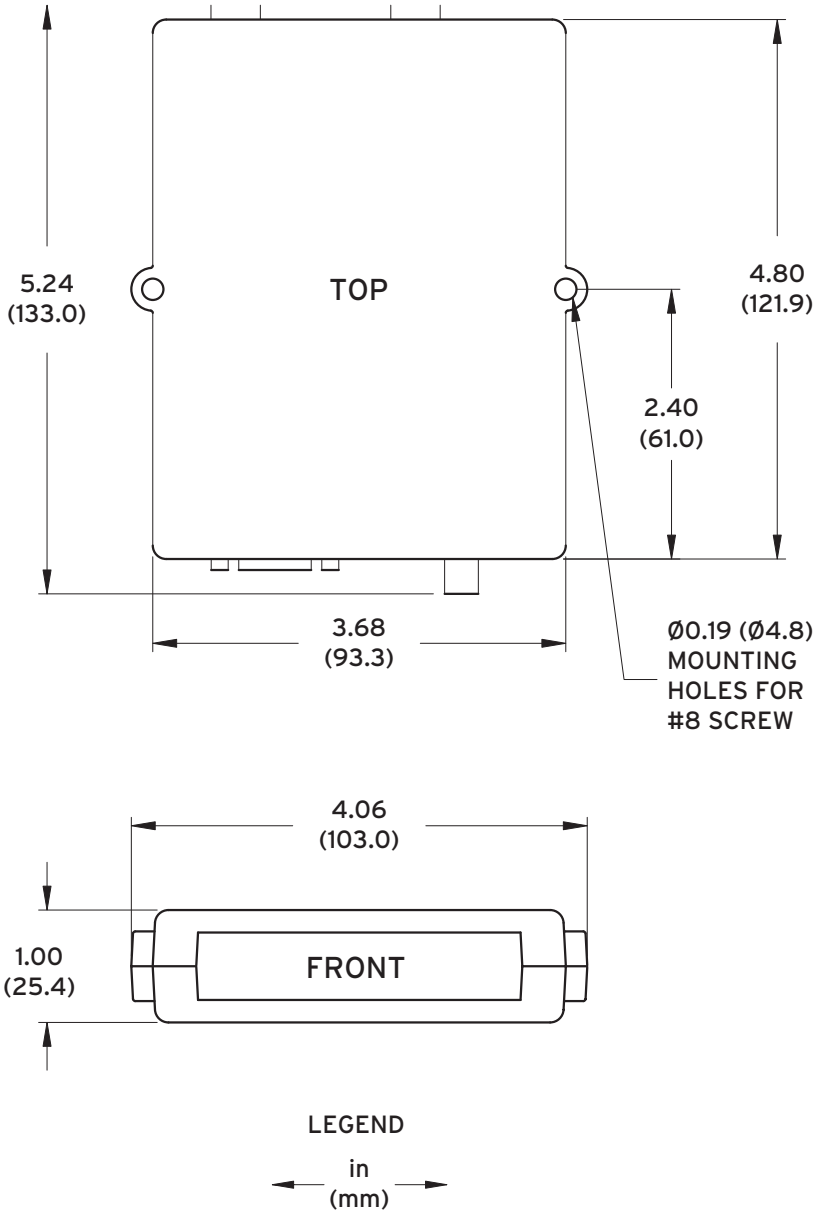

Figure 2.1 SEL-3022 Dimension Drawing

Preliminary Copy

Setting Up Your PC or PDA With the SEL-5809 and SEL-5810 Software

Software Installation

The SEL-5809 Settings Software is required to set, operate, and test the SEL-3022. The SEL-5810 Virtual Serial Software is used by operators to connect PC programs to remote IEDs using the SEL-3022. You can install the SEL-5809 and SEL-5810 Software on an IBM-compatible computer or a Pocket PC-compatible PDA. See *Software System Requirements on page 1.10 in Section 1: Introduction & Specifications*. If you have any difficulties installing the software, contact your customer service representative or the SEL factory for assistance.

The software will load automatically if the autorun feature is enabled on your computer; this is Method A. If autorun is not enabled on your computer, use the Windows **Run** command to load the software; this is Method B.

Perform the following steps to install the software:

Step 1. Load the software through use of one of the following methods:

- **Method A.** Load the software automatically.
  - To load the software automatically, make sure your PC is turned on and close all other applications.
  - Place the CD-ROM in the PC CD-ROM drive. The setup software should run automatically.
- **Method B.** Use the Windows **Run** command to load the software.
  - If the **Setup** program does not start automatically, use the Microsoft Windows **Run** function (from the **Start** menu) to load the software.
  - Type the command shown in *Figure 2.2*, being certain to use the correct drive letter for the CD-ROM drive in your PC (the CD-ROM drive in the example shown in *Figure 2.2* is drive D:\).

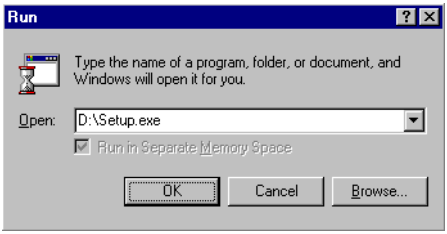

Figure 2.2 Windows Run Command

Preliminary Copy

Step 2. Complete the software loading process. Follow the loading instructions as they appear on the PC screen.

Registering the SEL-5809 Settings Software

To start the SEL-5809 Settings Software, use the Windows **Start** menu to open the software. If you installed the software within the Programs group in the main Windows directory, click **Start** > **Programs** > **SEL Applications**. If you used a custom program group, click **Start** > **Programs** > and the custom group.

You can also create a shortcut on the Windows Desktop. See your Windows documentation for instructions on creating a shortcut. Double-click the shortcut icon to start the software from the shortcut.

Before using the SEL-5809 Settings Software it must be registered. The product unregistered prompt message displays when you start the software. (See *Figure 2.3*.)

NOTE: To modify settings in the SEL-3022, an 802.11b WiFi interface is required on the PC or PDA. Install the SEL-5809 Settings Software on a PC or PDA with an 802.11b WiFi card.

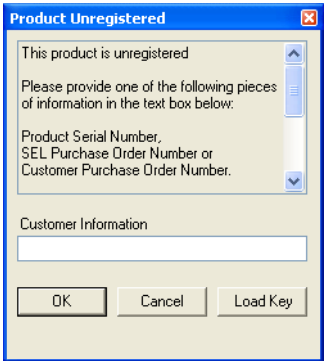

Figure 2.3 Product Unregistered Prompt

To register the SEL-5809 Settings Software, perform the following steps.

Step 1. At the prompt's text box enter the SEL-3022 Serial Number, SEL Purchase Order Number, or Customer Purchase Order Number.

Step 2. Click **OK**. This generates the registration file (reginfo.xml).

Step 3. Save the registration file (reginfo.xml) onto your computer in a location you can remember.

Step 4. Email the file to 5809@selinc.com or contact your customer service representative.

Preliminary Copy

Step 5. When SEL receives your e-mail, you will be sent a registration key file (regkey.xml), which allows you to run the SEL-5809 Settings Software.

Step 6. Once you receive this key file, save it on your computer.

Step 7. Restart the SEL-5809 Settings Software. Load the key file using the **{Load Key}** button of the registration form. The key automatically removes the lock.

NOTE: The registration form is also available using the **Help > Register** menu.

The SEL-5810 Virtual Serial Software does not have a registration key and does not need to be registered.

PDA Software Installation

This section assumes you have Microsoft ActiveSync installed on your computer. If you do not, consult your PDA manual or download a free version from Microsoft.

To install the PDA software to the PDA, perform the following:

Step 1. Connect the PDA to the ActiveSync cradle. This should activate the ActiveSync software.

Step 2. Install Compact Framework to the PDA.

Step 3. Launch the Pocket PC installation package from the SEL-5809 Settings Software or SEL-5810 Virtual Serial Software.

Step 4. To access the SEL-5809 Settings Software or SEL-5810 Virtual Serial Software, click on the icon in the programs menu of the PDA.

You must register the SEL-5809 Settings Software before you can use it. The product unregistered prompt message displays when you start the software.

To register the SEL-5809 Settings Software, perform the following steps.

Step 1. At the prompt's text box enter the SEL-3022 Serial Number, SEL Purchase Order Number, or Customer Purchase Order Number.

Step 2. Click **OK**. This generates the registration file (reginfo.xml).

Step 3. Save the registration file (reginfo.xml) onto your PDA in a location you can remember.

Step 4. Email the file to 5809@selinc.com or contact your customer service representative.

Step 5. When SEL receives your e-mail, you will be sent a registration key file (regkey.xml), which allows you to run the SEL-5809 Settings Software.

Step 6. Once you receive this key file, save it on your PDA.

Cryptographic Manual—Do Not Copy
Preliminary Copy

Step 7. Restart the SEL-5809 Settings Software. Load the key file using the **{Load Key}** button of the registration form. The key automatically removes the lock.

NOTE: The registration form is also available using the **Help > Register** menu.

The SEL-5810 Virtual Serial Software does not have a registration key and does not need to be registered.

Initializing the SEL-3022

When the SEL-3022 is sent from the factory, or if the **{RESET}** button in the SEL-3022 is pressed, the transceiver is in a Reset state. The Reset state indicates that all of the encryption keys and related security parameters are erased. You can quickly determine whether the SEL-3022 is in a Reset state by applying power and viewing the status LED. In the Reset state, the LED turns on and off at a two-second interval. When the SEL-3022 is in the Reset state, the wireless interface is disabled, and the DCE serial port is set to configuration mode. To initialize the SEL-3022, use the SEL-5809 Settings Software and configure the settings as defined in the following steps.

NOTE: Only the PC version of the SEL-5809 Settings Software can initialize the SEL-3022; the PDA version **cannot** initialize the SEL-3022.

Perform the following steps to initialize the SEL-3022:

Step 1. Connect a straight-through EIA-232 cable from the host computer serial port to the SEL-3022 DCE port.

Step 2. Apply power to the SEL-3022 (see *Power Supply Connections on page 1.6 in Section 1: Introduction & Specifications*).

Step 3. Start the SEL-5809 Settings Software.

Step 4. Select **File > New Device**, choose a device template from the **Select a Device Type to Create** box, press **Create**. *Figure 2.4* is an example.

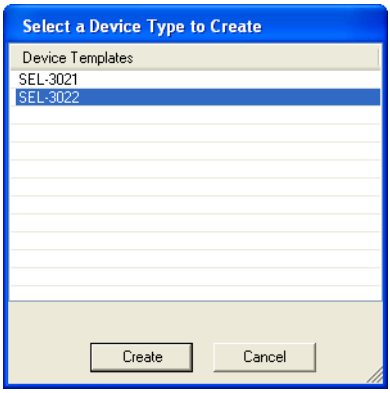

Figure 2.4 Select a Device Type to Create

Step 5. Type in the Device Location and Device Name. *Figure 2.5* is an example.

Figure 2.5 Specify New Device Location

Step 6. Click **OK**.

Step 7. Your device location is now listed. For our example, this location is New_Group. Select the plus arrow beside your new device location to expand the view.

Step 8. To open a serial connection to the SEL-3022, double-click on the device name. In our example, this name is Device 1.

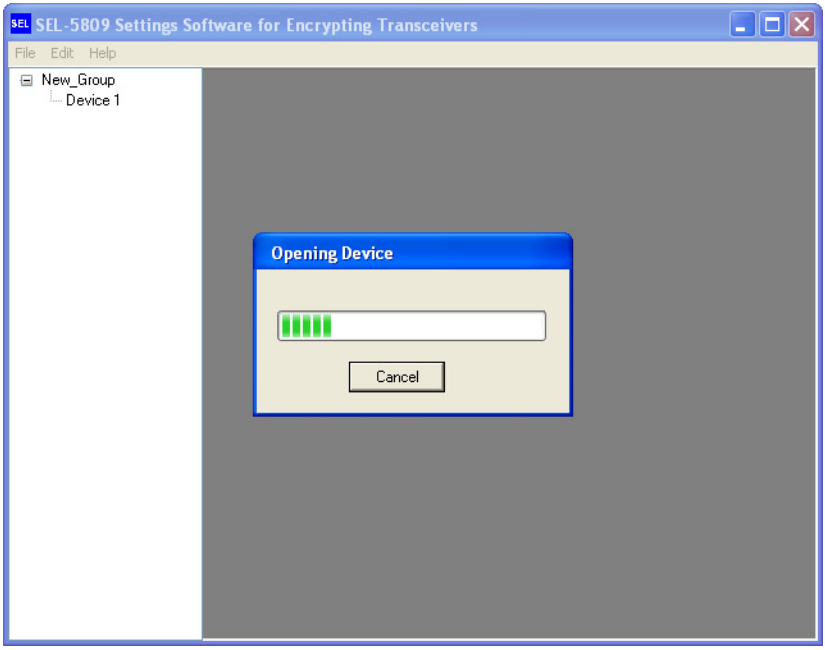

Figure 2.6 Opening Device

Step 9. The first screen displays your system parameters.

Figure 2.7 Identification Screen

Step 10. The **Status: Device** tab shows the SEL-3022 diagnostic status, previous diagnostic failures, and the constant transmit test feature. *Figure 2.8* is an example.

Refer to *Device Information on page 4.7 in Section 4: Settings and Commands* for a description of these test parameters. While the SEL-3022 is in the Reset state, the **Status: Device** tab allows the user to constantly transmit data on a selected 802.11b channel. This feature may be used to test the SEL-3022 wireless propagation characteristic at an installation site.

NOTE: The constant transmit test function is only available in the Reset state. After the SEL-3022 is initialized, this feature is no longer available.

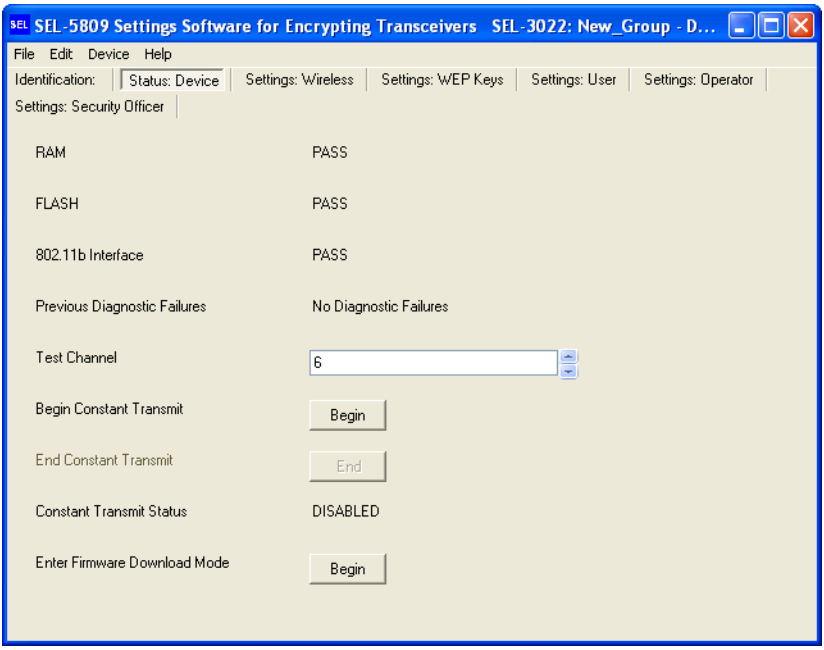

Figure 2.8 Status: Device

Step 11. Select the **Settings: Wireless** tab and consult your System Administrator for the Wireless Connections Settings. The settings shown are for example only.

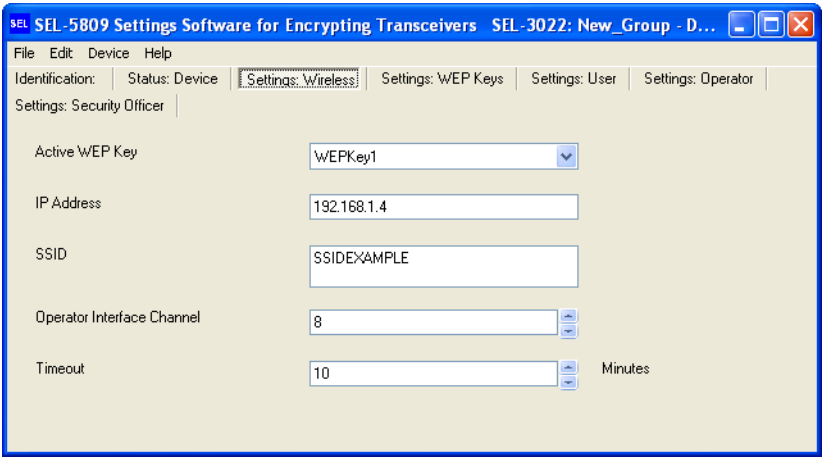

Figure 2.9 Settings: Wireless

Step 12. Select the **Settings: WEP Keys** tab and consult your System Administrator for the WEP Key Settings. The settings shown in *Figure 2.10* are for example only. WEP Keys must be set to a unique 26-character hexadecimal ASCII value other than the default.

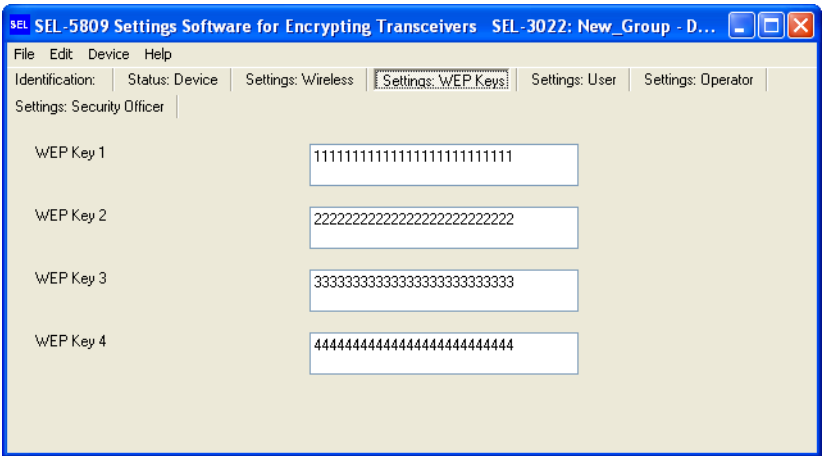

Figure 2.10 Settings: WEP Keys

Step 13. Select the **Settings: User** tab and enter random 32-character hexadecimal ASCII encryption and authentication keys. Select a password or phrase that is 6–60 characters in length. Only the security officer should set the encryption and authentication keys. All values must be set to nondefault values. The settings shown in *Figure 2.11* are for example only.

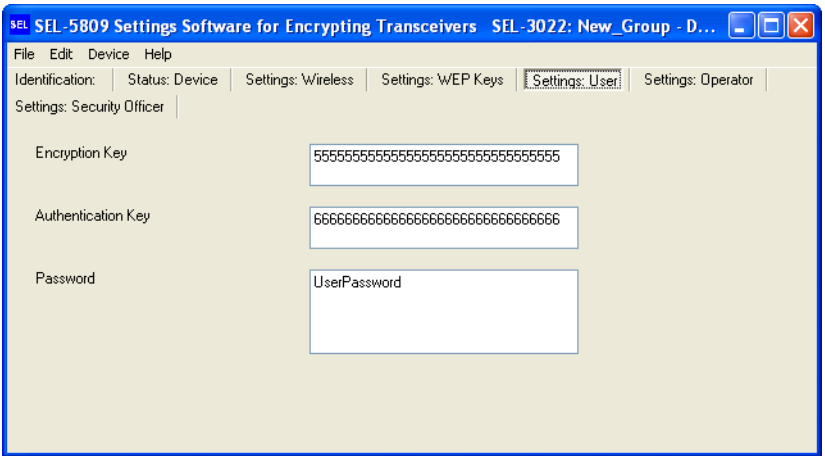

Figure 2.11 Settings: User

Step 14. Select the **Settings: Operator** tab and enter random 32-character hexadecimal ASCII encryption and authentication keys. Select a password or phrase that is 6–60 characters in length. Only the security officer should set the encryption and authentication keys. All values must be set to nondefault values. The settings shown in *Figure 2.12* are for example only.

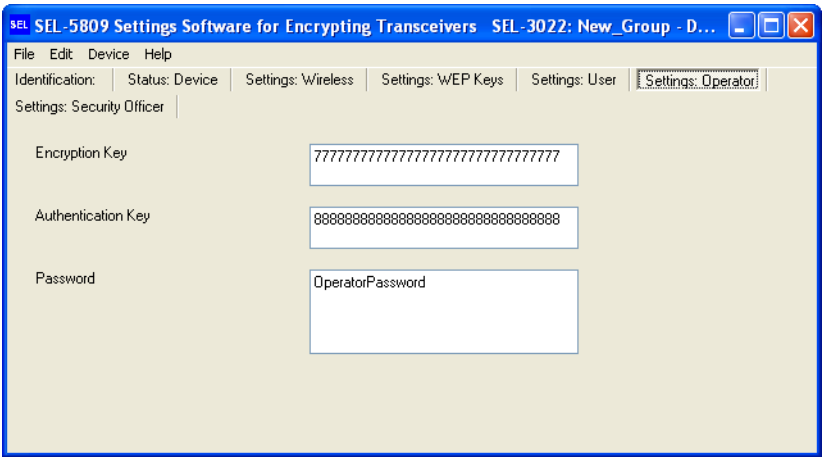

Figure 2.12 Settings: Operator

Step 15. Select the **Settings: Security Officer** tab and enter random 32-character hexadecimal ASCII encryption and authentication keys. Select a password or phrase that is 6–60 characters in length. Only the security officer should set the encryption and authentication keys. All values must be set to nondefault values. The settings shown in *Figure 2.13* are for example only.

NOTE: The security officer keys cannot be the same as the operator keys.

Figure 2.13 Settings: Security Officer

Step 16. After you are satisfied with your choices select **Device** > **Send All**. This will send your initialization settings to the SEL-3022.

Step 17. You will see the following confirmation of send prompt. Select **Yes** to continue or **No** to abort.

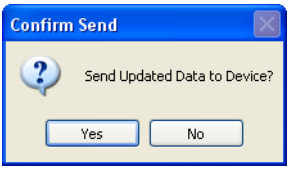

Figure 2.14 Confirm Send Prompt

Step 18. When settings have been sent successfully the following pop-up message appears. Select **OK** to acknowledge the message.

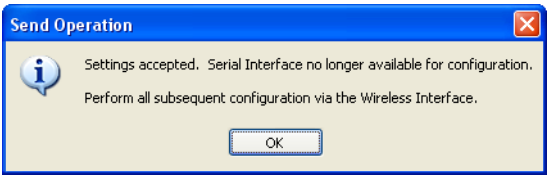

Figure 2.15 Send Operation Message

Step 19. Verify that the Status LED on the SEL-3022 is illuminated. If all settings were configured to valid values, the SEL-3022 is now initialized. The Status LED will be illuminated, and you can use the 802.11b wireless interface to configure the SEL-3022 for your application.

Step 20. You should record the settings and store them in a secure place. To do this, select **File** > **Print**, choose the settings you want to print by placing a check mark beside them, and click **Print**. See *Figure 2.16*.

NOTE: In order to print the settings, they first must be sent to the device, as shown in Step 16.

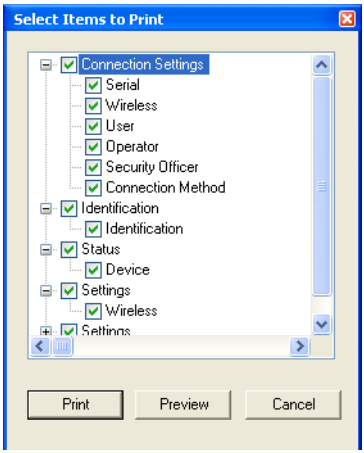

Figure 2.16 Select Items to Print

Step 21. Print to a specific printer or print directly to a file.

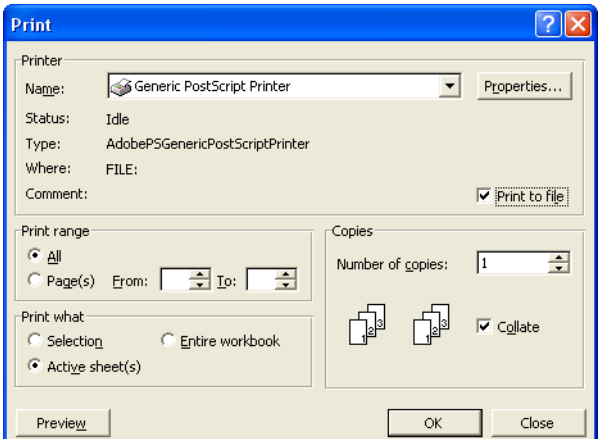

Figure 2.17 Print Window

Step 22. Close the Device by clicking **File** > **Close Device**. Select **Yes** when prompted to save current session.

Step 23. To open a wireless connection to the SEL-3022, double click on the device name. Select **User**, **Operator**, or **Security Officer**. Enter pass phrase, then click **OK**. The pass phrase that you enter must match the user, operator, or security officer password programmed during device initialization.

Wireless Configuration

A wireless card is required to perform in-system settings modifications, monitoring, and to establish a virtual serial port connection. The SEL-3022 complies with the IEEE 802.11b Wireless Standard. Suitable wireless cards and associated software drivers can be found at your local computer or office supply store.

Follow the 802.11b manufacturer's installation procedure (for either the PC Wireless Card or a PDA) to install the wireless card.

After the wireless card is installed, you must enable Wired Equivalence Protocol (WEP—see *Appendix C: Wireless Operator Interface Security* for details). Open the 802.11b wireless driver and locate the security settings. Enter all WEP keys, including the active WEP key. The WEP keys on your PC or PDA must match the WEP keys the SEL-5809 Settings Software loaded during SEL-3022 initialization.

Preliminary Copy

This page intentionally left blank

Preliminary Copy

Section 3

Job Done Example

Introduction

This section contains a Job Done® example for applying the SEL-3022 to an SEL-651R Recloser Control mounted twenty feet above the street.

Job Done Example 1

EXAMPLE 3.1 Applying the SEL-3022 to an SEL-651R

Identifying the Problem

Your objective is to provide a simple and secure means of communications to an SEL-651R Recloser Control mounted twenty feet above the street. You decide on the SEL-3022 Wireless Encrypting Transceiver for the following reasons:

- The SEL-3022 eliminates the requirement to have physical access to the recloser control, i.e. you do not need a bucket truck to get close enough to communicate with the SEL-651R.
- The SEL-3022 protects wireless data with IEEE 802.11b WEP encryption in addition to the 128-bit AES and HMAC SHA-1 cryptographic security it provides. This is perfect for protecting passwords and other sensitive information.
- The SEL-5809 Settings Software and SEL-5810 Virtual Serial Software allow you to continue to use all of your standard PC software programs to communicate, set, and analyze data from the recloser control.
- The installation is simple and the antenna fits in a standard 3/4-inch knockout in the bottom of the recloser control.

Defining the Solution

Figure 3.1 represents the recloser control. Your task is to configure and install the SEL-3022.

Figure 3.1 Remotely Located Recloser Control

SEL-3022 Initialization

An SEL-3022 direct from the factory is in a Reset condition. You must initialize various settings before installing the SEL-3022 in the recloser control. You can initialize the SEL-3022 at your desk before you deploy the transceiver.

You will need the following:

- PC with IEEE 802.11b wireless card and SEL-5809 Settings Software loaded.
- SEL-C388 cable, or equivalent - used to initialize the SEL-3022.
- SEL-C387 cable or equivalent - installed between the SEL-3022 and SEL-651R.
- SEL-651R or equivalent.
- ACSELERATOR or other serial port program (e.g., HyperTerminal®).

Follow the instructions for Initializing the SEL-3022 on page 2.7 in Section 2: Installation, to set up and initialize the SEL-3022.

Set the Device Location and Device Name to Pole 43 and SEL-651R, respectively. Figure 3.2 shows the SEL-5809 Settings Software top level view for this example.

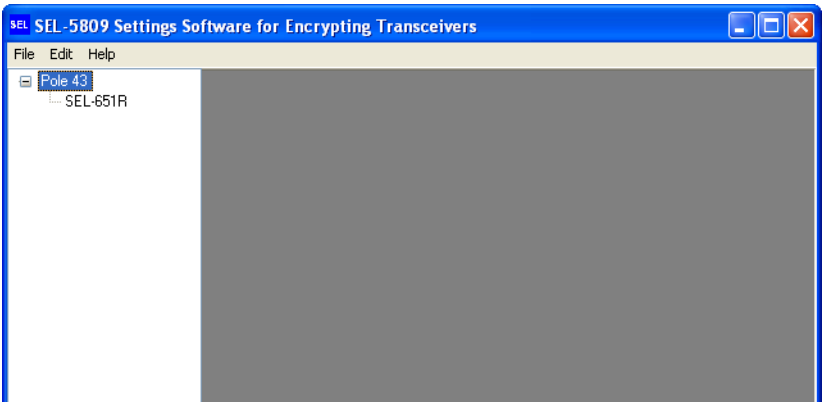

Figure 3.2 Job Done Example SEL-5809 Top Level View

SEL-3022 Configuration Settings

Step 1. Open the SEL-5809 Settings Software.

Step 2. Select **Pole 43** (as configured above).

Step 3. Double-click on **SEL-651R**.

Step 4. Select **Security Officer** and enter your pass phrase. (See Figure 3.3.)

Step 5. Click **OK**.

Figure 3.3 Select a Wireless Session for DNP3 Job Done Example

Step 6. Select the **Settings: DCE Port** tab and configure the serial port parameters to match the SEL-651R serial port which the SEL-3022 is going to be connected to.

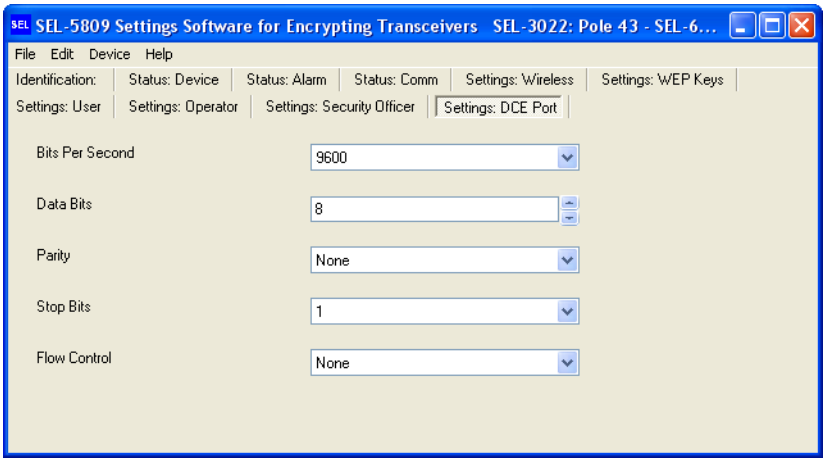

Figure 3.4 Settings: DCE Port

Step 7. Select **Device > Send All** to save the settings to the SEL-3022.

Step 8. Select **File > Close Device** to close the connection to the SEL-3022.

Step 9. Connect a C387 (or equivalent cable) between the SEL-3022 and SEL-651R.

Step 10. Through use of the SEL-5809 Settings Software select **Pole 43**.

Step 11. Double-click **SEL-651R**.

Step 12. Select **User** and enter your pass phrase. The following tab will be displayed.

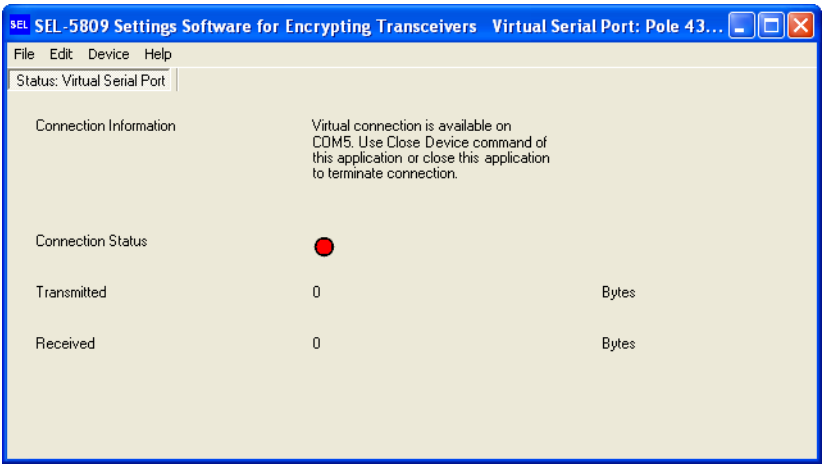

Figure 3.5 Status: Virtual Serial Port With Connection Status Red

NOTE: This display informs you regarding the virtual serial port number created by the SEL-5809 Settings Software. In this case, the SEL-5809 Settings Software has created COM5. Also note the Connection Status is RED indicating that there is not a PC program using the virtual port.

Step 13. Open ACSELERATOR (or other serial terminal program).

Step 14. Select **Communication > Parameters** and set Device to the virtual serial port that the SEL-5809 Settings Software created.

Step 15. Select **OK**. See Figure 3.6.

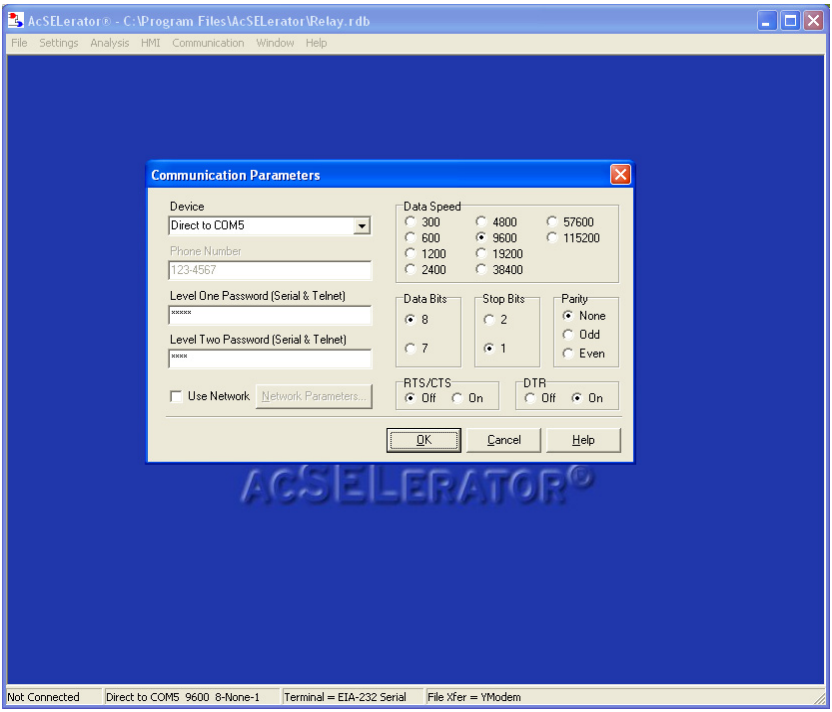

Figure 3.6 Communication Parameters Window in ACSELERATOR

16. At this point, a virtual connection between ACSELERATOR and the SEL-651R exists. Look at the SEL-5809 Settings Software **Status: Virtual Serial Port** page, the Connection Status is GREEN indicating the virtual serial port is in service.

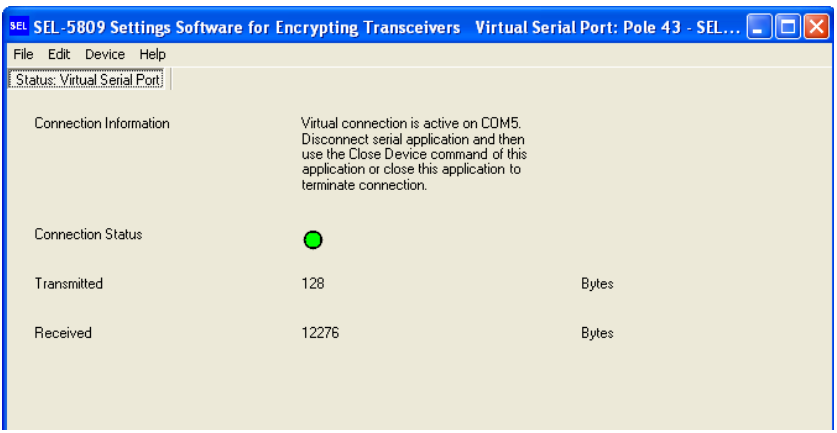

Figure 3.7 Status: Virtual Serial Port With Connection Status Green

Step 17. Through use of ACSELERATOR, you can perform such tasks as reading the settings out of the SEL-651R (see Figure 3.8) or viewing the metering data (see Figure 3.9).

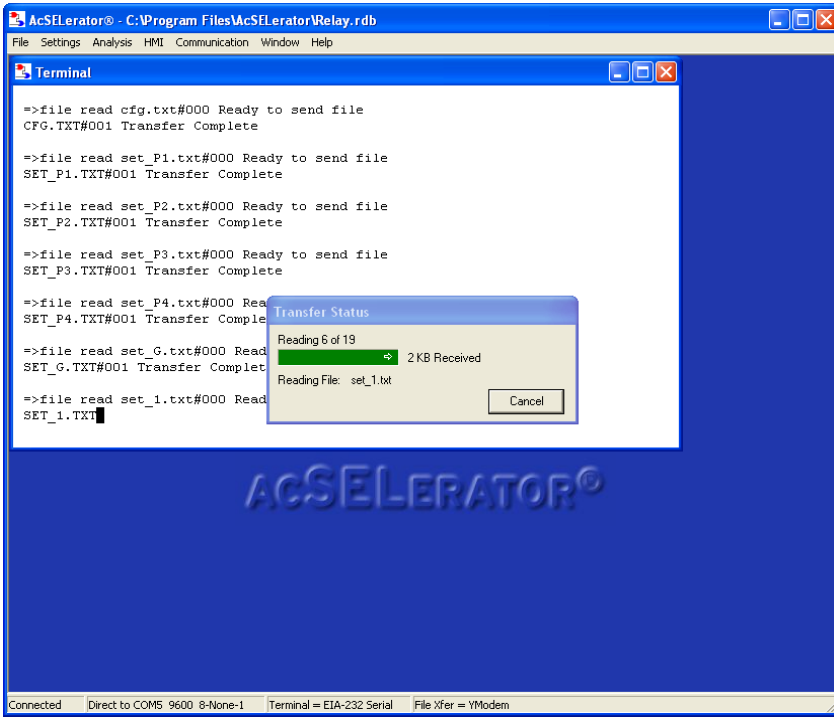

Figure 3.8 Reading Settings Via the SEL-3022

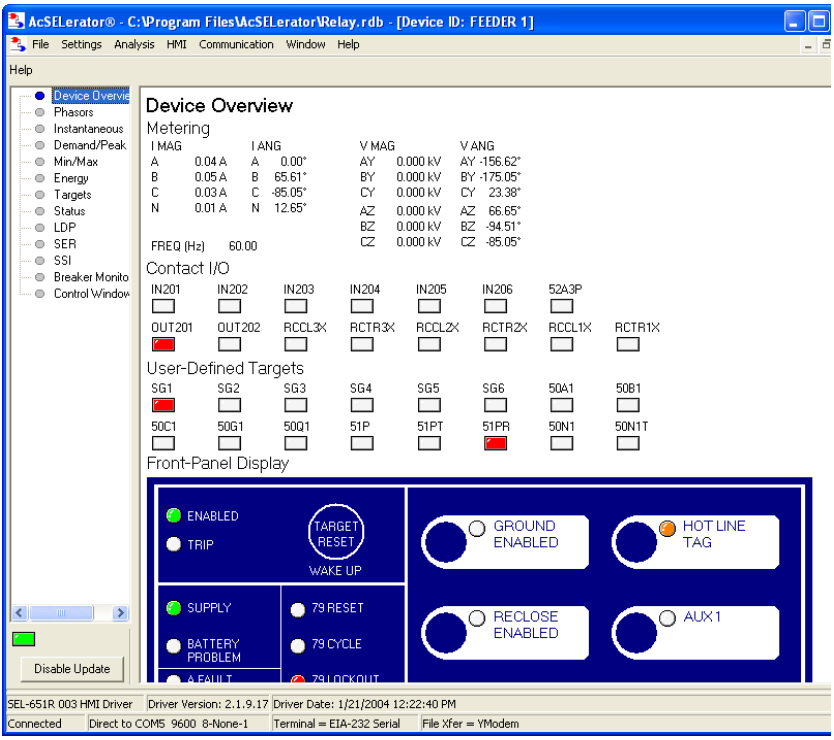

Figure 3.9 Monitoring SEL-651R Meter Data Via the SEL-3022

Step 18. When you are done setting and configuring the SEL-651R, click **Communication > Disconnect** (to close the ACSELERATOR serial port connection) or click **File > Exit** (to shut down ACSELERATOR).

NOTE: After you perform this operation, the Status: Virtual Serial Port Connection Status LED in the SEL-5809 Settings Software, will return to RED, indicating the virtual serial port is no longer being used by a PC program. See Figure 3.10.

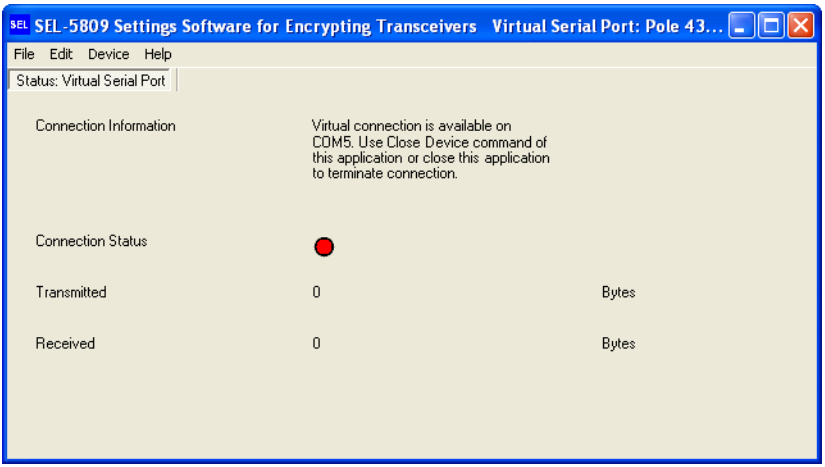

Figure 3.10 Status: Virtual Serial Port Connection Status Red

Step 19. Select **File > Close Device**, to close the SEL-5809 Settings Software virtual serial port.

Linemen or engineers who do not need to configure the SEL-3022 transceivers, will use the SEL-5810 Virtual Serial Software, which is strictly a virtual serial port program. Use the SEL-5809 Settings Software to generate the configuration files for the SEL-5810 Virtual Serial Software that contain all of the configuration parameters necessary to establish a connection between a PC and SEL-3022.

To generate a user file for a lineman's PC complete the following steps.

Step 20. Select **File > Export** in the SEL-5809 Settings Software.

Step 21. Check the **User** box next to **Pole 43/SEL-651R** device. Refer to Figure 3.11.

Step 22. Select **SEL-5810** from Format drop-down menu. Refer to Figure 3.11.

Step 23. Select the **{Export}** button.

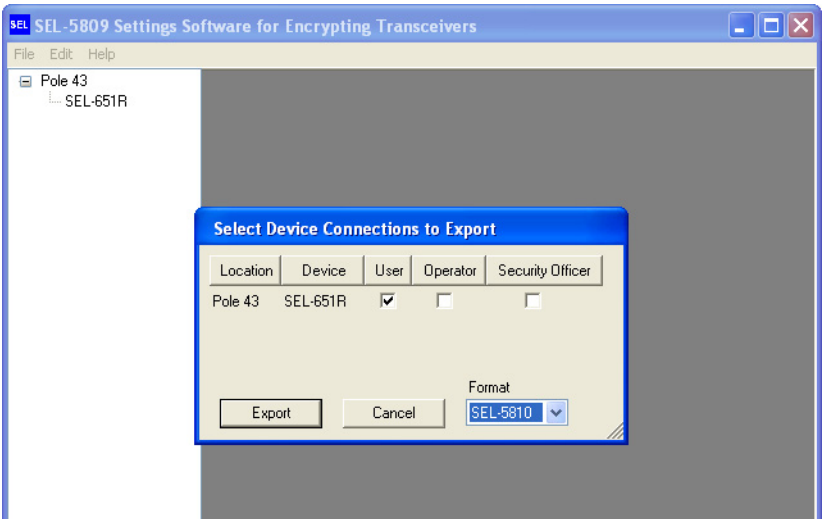

Figure 3.11 Specify Device to Export to SEL-5810 Virtual Serial Software

Step 24. Enter an encryption password to protect the file.

Step 25. Select **OK**. This will keep the file encrypted while it is being transferred to the lineman's PC.

Figure 3.12 Export Encrypted User Configuration File

Step 26. Choose a folder to store the encrypted file and enter a file name in the **File name** box.

Step 27. Select **OK**. This saves the file to the location specified by Step 26.

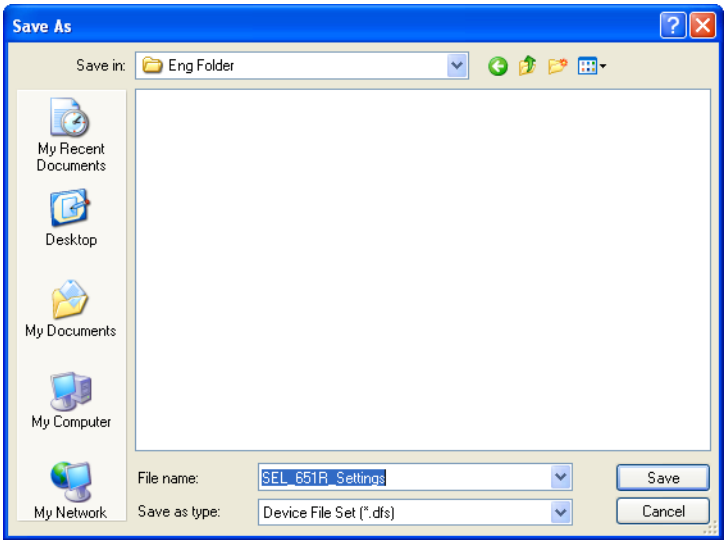

Figure 3.13 Store Encrypted File

Step 28. Send or load this file onto the lineman's PC.

Step 29. Start the SEL-5810 Virtual Serial Software.

Step 30. Click **File > Import** and select the file saved in Step 26 to import the SEL-3022 device image into the SEL-5810 Software.

Step 31. Enter password.

Step 32. Select **OK**.

Step 33. Select the **{Connect}** button.

Step 34. Enter User password.

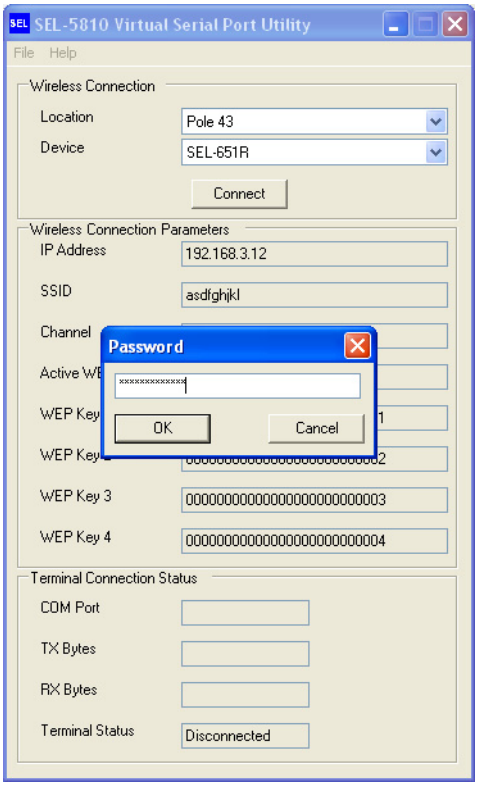

Figure 3.14 Password Prompt in SEL-5810 Virtual Serial Software

Step 35. Verify the **{Connect}** button changes from **Connect** to **Disconnect**.

Step 36. Open ACSELERATOR.

Step 37. Select **Communication < Parameters**.

Step 38. Specify Device by selecting, from the drop-down menu, the Communication port generated by the SEL-5810 Virtual Serial Software (reference the SEL-5810 **Terminal Connection Status: COM Port**).

Step 39. Select **OK**.

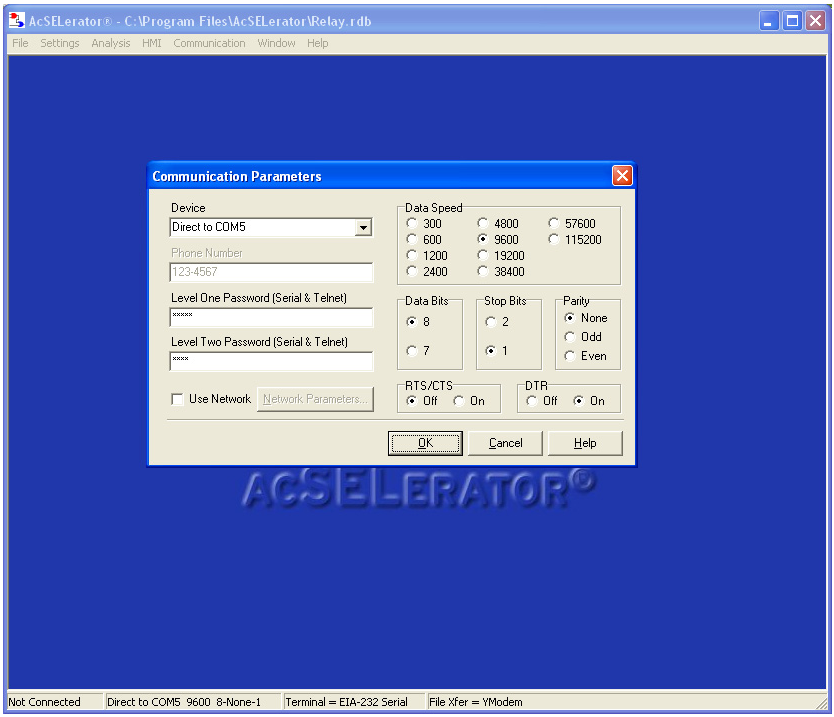

Figure 3.15 Communication Parameters Window in ACSELERATOR

Step 40. Verify on the SEL-5810 the **Terminal Connection Status: Terminal Status** shows **Connected**.

Step 41. You can now perform setting and monitoring functions via the ACSELERATOR program such as reading SER reports by selecting **HMI < Meter & Control < SER**.

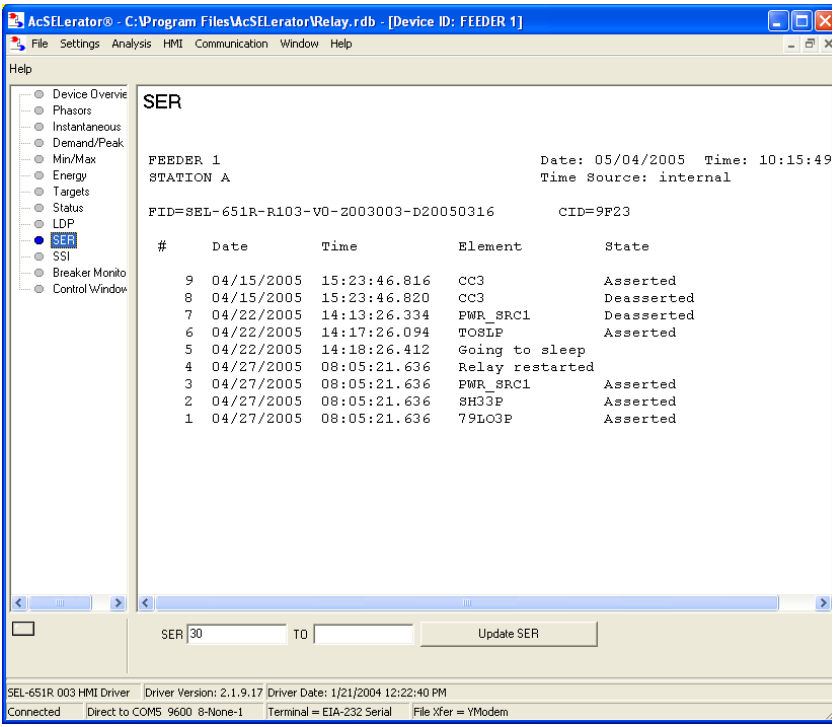

Figure 3.16 Reading SER Report Via ACSELERATOR

Step 42. When you are done communicating with the SEL-651R, close ACSELERATOR.

Step 43. At that point the SEL-5810 **Terminal Connection Status: Terminal Status** shows **Disconnected**.

Step 44. Select the SEL-5810 **Wireless Connection: {Disconnect}** button to close the wireless session. Note, the **{Disconnect}** button will change to **Connect**.

NOTE: The SEL-5810 Virtual Serial Software requires that the user's communications program, i.e., ACSELERATOR or HyperTerminal, close or disconnect the virtual serial port before it is possible to close the SEL-5810 Virtual Serial Software itself.

Preliminary Copy

Section 4

Settings and Commands

Introduction

This section explains the settings and commands of the SEL-3022.

- Serial Port Settings: Settings that configure the EIA-232 serial port.
- Wireless Port Settings: Settings that configure the 802.11b wireless port.
- Communication Status Command: Diagnostic status report on the health of the SEL-3022 serial port communications channel.
- Device Information: Displays device-related information.

Serial Port Settings

The following settings in *Table 4.1* configure the serial port.

Table 4.1 Settings: DCE Port

Setting Name	Setting Description	Value or Range
Bits Per Second	Serial Port Baud Rate in Bits per Second	300, 1200, 2400, 4800, 9600, 19200, or 38400
Data Bits	Number of data bits in serial port data format	6, 7, or 8
Parity	Parity mode of the serial port	Odd, Even, or None
Stop Bits	Number of stop bits in the serial port	1 or 2
Flow Control	Selects hardware flow control	Hardware or None

The SEL-3022 Universal Asynchronous Receiver/Transmitters (UARTs) have a one-character receive buffer. If the SEL-3022 asserts Hardware (HW) flow control, one additional character can be sent to the SEL-3022 without loss of data. If HW flow control is asserted and characters are still being sent to the SEL-3022 (e.g., from the serial port of a device connected to the SEL-3022) then characters will be lost.

Wireless Port Settings

The following settings configure the wireless interface.

NOTE: If the SEL-3022 is in a Reset mode, the wireless port will not function. See Initializing the SEL-3022 on page 2.7 in Section 2: Installation for details on enabling the wireless interface.

Table 4.2 Settings: Wireless

Setting Name	Setting Description	Value or Range
Active WEP Key	Selects which key will be used for the WEP encryption.	WEP Key 1, WEP Key 2, WEP Key 3, or WEP Key 4
IP Address	Internet Protocol address of wireless device. Consult your system administrator for an appropriate IP address.	1.0.0.0 to 255.255.255.255
SSID	Service Set ID of the wireless device. Consult your system administrator for an appropriate SSID value.	1–32 characters
Operator Interface Channel	Wireless radio channel. Consult your system administrator for an appropriate radio channel.	1–11
Timeout	Wireless timeout for TCP connection in minutes. The SEL-3022 closes the connection if no data is received after the specified length of time. (Recommendation: 10 min.) IMPORTANT: If you lose the wireless connection to the SEL-3022, the SEL-3022 will not accept a new connection until the timeout period expires.	1–15 minutes

NOTE: Contact your network administrator for a valid IP address.

WEP Key settings configure WEP keys used by the SEL-3022 wireless mode. The WEP key used in the SEL-3022 wireless module must match those used in your PC or PDA.

Table 4.3 Settings: WEP Keys

Setting Name	Setting Description	Value or Range
WEP Key 1	Twenty-six character hexadecimal (104-bit) key used in the wireless encryption algorithm.	0–9 and A–F
WEP Key 2	Twenty-six character hexadecimal (104-bit) key used in the wireless encryption algorithm.	0–9 and A–F
WEP Key 3	Twenty-six character hexadecimal (104-bit) key used in the wireless encryption algorithm.	0–9 and A–F
WEP Key 4	Twenty-six character hexadecimal (104-bit) key used in the wireless encryption algorithm.	0–9 and A–F

The SEL-3022 provides three login roles on the wireless interface. The **User** role allows EIA-232 to 802.11b wireless communication. SEL-3022 parameters cannot be changed in the **User** role.

The **Operator** role provides read and write privileges on all settings except those that may compromise the security of the device (encryption and authentication keys, access passwords, settings that may disable critical security functions, etc.). In addition, the **Operator** login role can access all of the SEL-3022 diagnostics capabilities.

The **Security Officer** login role provides a slightly higher access privilege by allowing all of the actions provided by the **Operator** login role, plus the ability to write new values to all cryptographic security parameters and sensitive settings. The three individual roles are authenticated on the wireless operator interface using a completely separate set of login authentication parameters.

There is an Encryption Key, Authentication Key, and Password associated with each login role. The values of each of these three settings must be different for each of the three roles.

Table 4.4 Settings: User

Setting Name	Description	Value or Range
Encryption Key	Thirty-two character hexadecimal ASCII (128-bit) key.	0–9 and A–F
Authentication Key	Thirty-two character hexadecimal ASCII (128-bit) key.	0–9 and A–F
Password	Password or Pass Phrase for user-controlled access, referred to as Access Level 1.	6–80 printable ASCII characters

Table 4.5 Settings: Operator

Setting Name	Setting Description	Value or Range
Encryption Key	Thirty-two character hexadecimal ASCII (128-bit) key.	0–9 and A–F
Authentication Key	Thirty-two character hexadecimal ASCII (128-bit) key.	0–9 and A–F
Password	Password or Pass Phrase for operator-controlled access, referred to as Access Level 1.	6–80 printable ASCII characters

Table 4.6 Settings: Security Officer

Setting Name	Setting Description	Value or Range
Encryption Key	Thirty-two character hexadecimal ASCII (128-bit) key.	0–9 and A–F
Authentication Key	Thirty-two character hexadecimal ASCII (128-bit) key.	0–9 and A–F
Password	Password or Pass Phrase for security officer access, referred to as Access Level 2.	6–80 characters

IMPORTANT: The user, operator, and security officer passwords cannot be read out of the SEL-3022 with the SEL-5809 Settings Software or SEL-5810 Virtual Serial Software. Record the keys and passwords in a safe place. If you lose keys or passwords, you must reset and initialize the SEL-3022 with new values before you can modify settings.

NOTE: The security officer, operator, and user security settings cannot be the same. If any of the security settings are the same for the user, operator, and security officer settings, the SEL-5809 Settings Software will generate an error.

Communication Status Command

You can use the SEL-5809 Settings Software and the wireless interface to issue a Communication Status command. Use the Communication Status command to analyze the health of your serial channel. All error counters reset to zero when you press the Clear Comm Statistics **{Clear}** button or if power is cycled to the SEL-3022. The Communication Status includes the following information:

Table 4.7 Status Command Names and Descriptions

Status	Status Name	Description
DCE Serial Port Errors	DCE Framing Errors	Number of times a Stop Bit failure has occurred.
	DCE Overrun Errors	Number of times a receive character was not removed from the serial port before a new character has arrived.
	DCE Parity Errors	Number of times a parity error has occurred.
	DCE Error Total	Total number of Framing, Overrun, and Parity Errors.
Contact Alarm Comm Pulse	How much any communications statistics value must increase before pulsing the alarm contact.	0–500 Failures
Clear Comm Statistics (Button)	NA	Press to clear all communication statistics to zero.

Device Information

You can use the SEL-5809 Settings Software and the wireless interface to obtain device information.

Table 4.8 Identification

Version Name	Version Description
Firmware Version	This is the released firmware version number the SEL-3022 is running.
Hardware Version	This is the released hardware version number that determines the SEL-3022 configuration.
Firmware Download #	Datecode indicating the date and numbered programming of the device.
MAC Address (See Specifications)	The 802.11b wireless interface Media Access Control address. This is a unique address.

Device Status

You can use the SEL-5809 Settings Software to determine the SEL-3022 self-test status and wireless module signal strength.

Table 4.9 Status: Device

Test/Comm Quality	Status	Description
RAM	PASS or FAIL	Indicates status of RAM tests
FLASH	PASS or FAIL	Indicates status of FLASH tests
802.11b Interface	PASS or FAIL	Status of wireless module interface
Comm Quality	dB	The Signal to Noise level
Avg Signal Level	dBm	Received power level of wireless module
Avg Noise Level	dBm	Received noise level of wireless module
Previous Diagnostic Failures	Status of last four diagnostic failures	Shows the most recent four diagnostic failures and associated diagnostic information

Output Alarm

Use the SEL-5809 Settings Software to test the alarm output of the SEL-3022.

Table 4.10 Status: Output Alarm

Name	Display	Description
Alarm	Red = alarm contact is open White = alarm contact is closed	Indicates status of alarm contact
Pulse Duration	1–30	Number of seconds to pulse the alarm output
Pulse Alarm Contact	NA	Selecting Pulse will pulse (open) the alarm output for the Pulse Duration

Virtual Serial Port

The **Status: Virtual Serial Port** view is only available in the **User** mode.

Table 4.11 Status: Virtual Serial Port

Name	Display	Description
Connection Information	Virtual connection is active on COMXX. Disconnect serial application and then use the **Close Device** command of this application or close this application to terminate connection	Indicates where a PC application can connect to the virtual serial port
Connection Status	Red = Not connected Green = Connected	Indicates when a PC application is connected to the virtual serial port
Transmitted	Number in Bytes	Number of bytes transmitted
Received	Number in Bytes	Number of bytes received

Preliminary Copy

Section 5

Testing and Troubleshooting

Introduction

This section provides guidelines for testing and troubleshooting the SEL-3022. Included are discussions on testing philosophies, methods, and tools. At the end of the section are descriptions of communication, channel diagnostics, self-tests, and troubleshooting procedures.

Testing Philosophy

SEL-3022 testing can be divided into three categories: acceptance, commissioning, and maintenance testing. The categories are differentiated both by when they take place in the life cycle of the transceiver and by test complexity. The paragraphs below describe when you should perform each type of test, the goals of testing at that time, and the functions that you need to test at each point.

This information is intended as a guideline for testing an SEL-3022.

Acceptance Testing

Perform acceptance testing when qualifying an SEL-3022 for use in a serial communication system that requires data encryption.

Goals of Acceptance Testing

- Ensure that the SEL-3022 meets published critical performance specifications.
- Ensure that the SEL-3022 meets the requirements of the intended application.
- Improve your familiarity with SEL-3022 capabilities.

What to Test

Acceptance test all setting parameters critical to your intended application.

SEL performs detailed acceptance testing on all SEL-3022 models and versions. Any SEL-3022 we ship meets published specifications. It is important for you to perform acceptance testing on an SEL-3022 if you are unfamiliar with SEL-3022 operating theory or settings. Such testing helps you ensure that SEL-3022 settings are correct for your application.

Commissioning Testing

Perform commissioning testing when installing a new SEL-3022 Serial Encrypting Transceiver.

Goals of Commissioning Testing

- Ensure that power connections are correct.
- Ensure that the Alarm Output connection is correct.

➤ Ensure that the SEL-3022 functions with your settings according to your expectations.

What to Test

Perform commissioning testing on serial, and wireless ports, and your alarm output.

SEL performs a complete functional check of each SEL-3022 before shipment. SEL-3022 commissioning tests should verify that the power supply, serial cable antenna, and alarm output (if used) are connected properly. Commissioning testing should also ensure proper configuration of the wireless interface.

Maintenance Testing

You generally do not need to perform maintenance testing on the SEL-3022. If you use the alarm output, you can use the SEL-5809 Settings Software **Pulse** command to verify functionality between the SEL-3022 and a connected device.

Cryptographic Manual—Do Not Copy
Preliminary Copy

Communications Channel Diagnostics

The SEL-3022 provides a serial communication diagnostic function to aid in troubleshooting.

The SEL-3022 monitors the DCE serial port for various errors. You can use the number and type of errors to troubleshoot communications channel problems. Use the SEL-5809 Settings Software Communications Channel Report page to retrieve communications channel diagnostics.

The SEL-3022 records the following Communications Channel Statistics.

Table 5.1 Status: Comm

Status	Status Name	Description
DCE Serial Port Errors	DCE Framing Errors	Number of times a Stop Bit failure has occurred.
	DCE Overrun Errors	Number of times a receive character was not removed from the serial port before a new character arrived.
	DCE Parity Errors	Number of times a parity error has occurred.
	DCE Error Total	Total number of Framing, Overrun, and Parity Errors.
Contact Alarm Comm Pulse	How much any communications statistics value must increase before pulsing the alarm contact	0–500 Failures
Clear Comm Statistics (Button)	NA	Press to clear all communication statistics to zero.

You can use the SEL-5809 Settings Software to clear comm statistics.

The wireless interface shows the Comm Quality (Signal-to-Noise ratio), Average Signal level in dBm, and Average Noise level in dBm. You can use these measurements to determine the wireless signal strength of the SEL-3022 as you apply the transceiver in your application.

Table 5.2 Device Status: Device Status (Sheet 1 of 2)

Status Name	Description
Comm Quality	Report RF Signal-to-Noise Ratio from 802.11b module

Preliminary Copy

Table 5.2 Device Status: Device Status (Sheet 2 of 2)

Status Name	Description
Avg Signal Level	Report RF Signal Level from 802.11b module
Avg Noise Level	Report RF Noise Level from 802.11b module

Self-Tests

The SEL-3022 has extensive self-test capabilities. You can determine the diagnostic status of your SEL-3022 via the SEL-5809 Settings Software or the Status LED located on the SEL-3022.

Table 5.3 SEL-3022 Self-Test Capabilities

Test	SEL-5809 Status: Device	SEL-3022 Disable	Status LED	Contact Output Alarm	Description
RAM	Pass	Yes	Toggle .5 second	Open	Performs a read and write verification
Flash	Pass	Yes	Toggle .5 second (if possible)	Open	Performs a checksum calculation
Crypto-graphic Algorithm Tests	NA	Yes	Toggle 1 second	Open	Checks known answer tests for all cryptographic func-tions
802.11b Self-Tests	NA	Yes	Toggle .5 second	Open	Indicates 802.11b wireless device health
802.11b SNR	dB	NA	NA	NA	Reports RF Signal-to-Noise Ratio from 802.11b module
802.11b Signal	dBm	NA	NA	NA	Reports RF Signal Level from 802.11b module
802.11b Noise	dBm	NA	NA	NA	Reports RF Noise Level from 802.11b module
RNG Test	NA	Yes	Toggle 1 second	Open	Compares each block with previous block
Zeroized Key	NA	Yes	Toggle 2 seconds	Open	Indicates presence of zeroized key material

Under normal operating conditions the contact alarm is closed. If the SEL-3022 is disabled the contact will open.

Troubleshooting

Inspection Procedure

Complete the following procedure before disturbing the SEL-3022. After you finish the inspection, proceed to the Troubleshooting Procedure.

Step 1. Measure and record the power supply voltage at the power input terminals.

Step 2. Check to see that the power is on. Do not turn the SEL-3022 off.

Step 3. Measure and record the voltage at the alarm output.

Step 4. Record the state of the Status LED, e.g., On, Off, or flashing rate.

Troubleshooting Procedure

Table 5.4 Troubleshooting

Condition of Status LED	Possible Cause/Response
Status LED is dark	Input power is not present or firmware has failed power on verification
Status LED is blinking at a flash rate of 0.5 seconds	The SEL-3022 has detected a hardware failure.
Status LED is blinking at a flash rate of 1 second	There is a problem with Cryptographic functions.
Status LED is blinking at a flash rate of 2 seconds	The SEL-3022 has been reset. Follow the initialization procedure to configure the device.
Status LED is on but unable to connect using wireless 802.11b interface	Verify that the Wireless channel, SSID, IP Address, WEP keys, Active WEP key, User/Operator/Security Officer key, and pass phrase are the same for both the SEL-5809 Settings Software and the SEL-3022. See *Initializing the SEL-3022 on page 2.7 in Section 2: Installation* for details.

Preliminary Copy

Factory Assistance

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 USA 99163-5603

Telephone: (509) 332-1890

Fax: (509) 332-7990

Internet: www.selinc.com

Preliminary Copy

Appendix A

Firmware and Manual Versions

Firmware

This manual covers SEL-3022 Wireless Encrypting Transceivers containing firmware bearing the firmware version numbers listed in *Table A.1*. This table also lists a description of modifications and the instruction manual date code that corresponds to firmware versions. The table lists the most recent firmware version first.

Table A.1 Firmware Revision History

Firmware Identification (FID) Number	Description of Changes	Manual Date Code
SEL-3022-R100-V0-Z001001-D20050615	Original Firmware Release.	20050615

Cryptographic Manual—Do Not Copy
Preliminary Copy

Instruction Manual

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

Table A.2 lists the instruction manual release dates and a description of modifications. The table lists the most recent instruction manual revisions at the top.

Table A.2 Instruction Manual Revision History

Revision Date	Summary of Revisions
20050615	Initial Release.

Preliminary Copy

Appendix B

Firmware Upgrade Instructions

Introduction

SEL occasionally offers firmware upgrades to improve the performance of your transceiver. The SEL-3022 stores firmware in Flash memory; therefore, changing physical components is not necessary. These instructions give a step-by-step procedure to upgrade the SEL-3022 firmware by uploading a file from a personal computer to the transceiver via the DCE serial port.

Required Equipment

You will need the following to perform a firmware upgrade:

- Personal computer (PC)
- SEL-5809 Settings Software
- Terminal emulation software that supports the Xmodem 1K protocol (these instructions use HyperTerminal® from a Microsoft® Windows® operating system)
- SEL-C388 Serial Cable or equivalent DCE to DTE "straight-through" cable capable of supporting hardware flow control
- The firmware upgrade file received from your SEL customer service representative

Upgrade Procedure

Perform the following steps to upgrade the SEL-3022 firmware:

Step 1. Record all settings if they are to be used after the upgrade. Typically, the previous session saves all but the cryptographic keys from the previous connection session. Right-clicking on the device will allow you to view the previous device image settings.

Step 2. If the SEL-3022 is in service, disconnect the cable connected to the DCE serial port.

IMPORTANT: Pressing the **{Reset}** button will erase all settings, so be sure to save your settings if they are going to be used again.

Step 3. Press the **{Reset}** button for at least 2 seconds. The Status LED will blink at a 2-second rate while in the reset mode.

Step 4. Start the SEL-5809 Settings Software and connect to the SEL-3022 via the serial port.

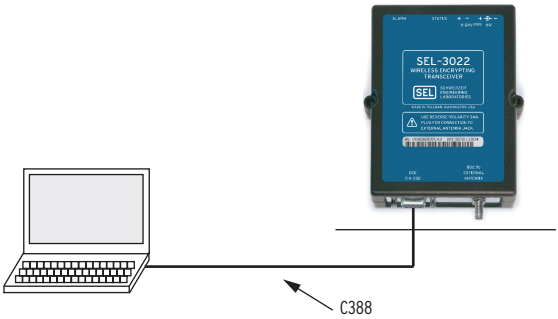

Figure B.1 PC to SEL-3022 Connection

NOTE: If you are upgrading a previously installed SEL-3022, right-click on the device name and select **Edit Connection Parameters**.

Step 5. At the **Serial** tab, select the serial port the PC will use to communicate with the SEL-3022.

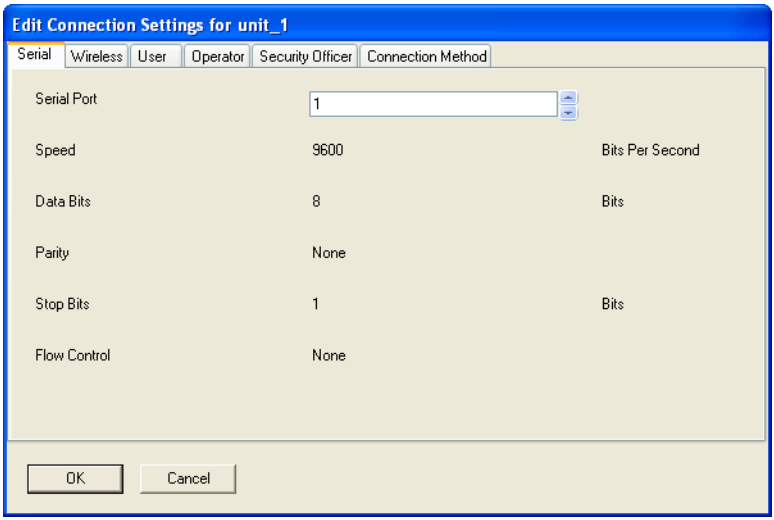

Figure B.2 SEL-3022 and SEL-5809 Connection Parameters

Step 6. At the **Connection Method** tab, select **Serial**.

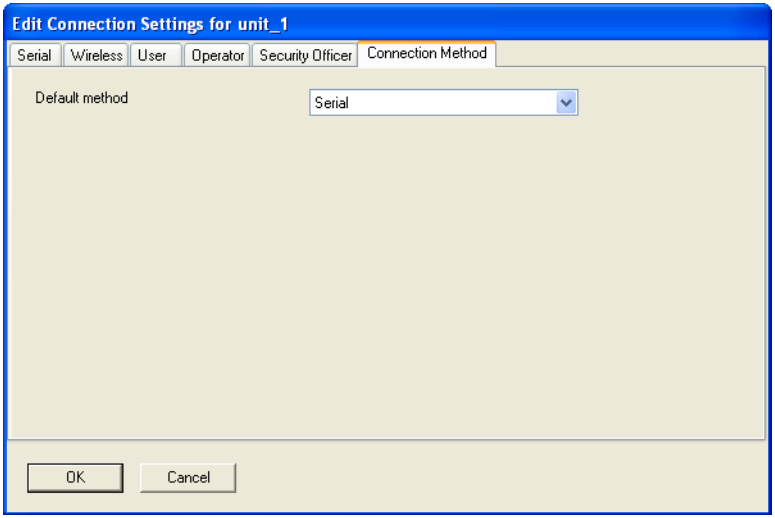

Figure B.3 SEL-5809 Settings Software Connection Method

Step 7. Click **OK**.

Step 8. Double-click the device from the SEL-5809 Settings Software main menu to establish communications. While the SEL-5809 Settings Software and SEL-3022 are establishing a connection you will see the following status box.

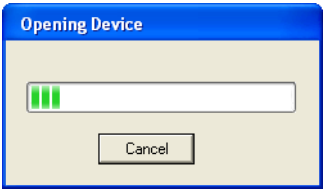

Figure B.4 SEL-5809 Opening Connection

Step 9. When the PC and SEL-3022 have established a connection, select the **Status: Device** tab.

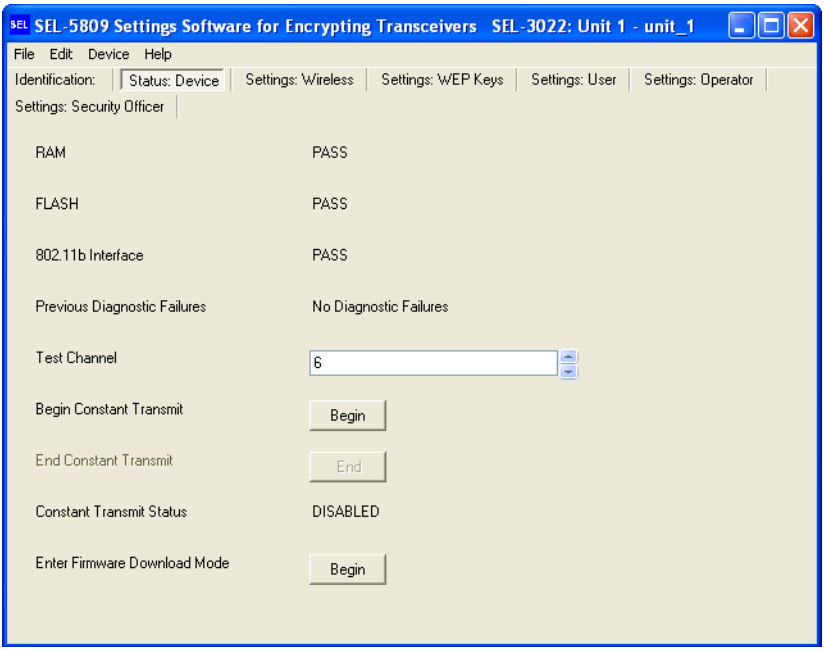

Figure B.5 Status: Device Window

Step 10. Click the **{Begin}** button to put the SEL-3022 into Firmware Download Mode.

Step 11. Click **Yes** to enter firmware download mode.

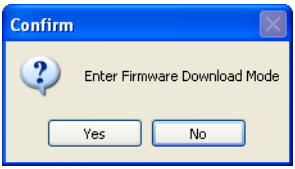

Figure B.6 Confirmation Prompt

Step 12. Click **OK** to acknowledge the SEL-3022 is entering firmware upgrade mode.

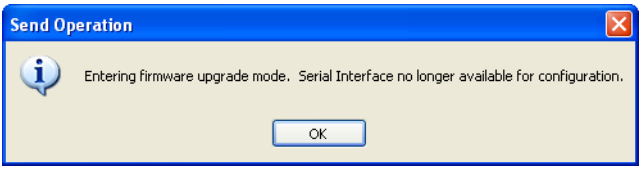

Figure B.7 Send Operation Prompt

Step 13. Configure the serial port settings in the Terminal software to the following:

a. Bits per Second: 115200

b. Data bits: 8

c. Parity: None

d. Stop bits: 1

e. Flow control: Hardware

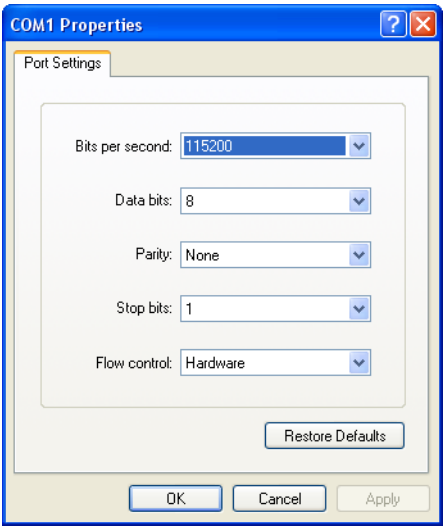

Figure B.8 Configuring Serial Port Settings in the Terminal Software

Step 14. Establish a connection to the SEL-3022 using the Terminal application.

Step 15. The SEL-3022 will send your Terminal a "C" indicating it is ready to commence an **Xmodem 1K** file transfer.

NOTE: The SEL-3022 will remain in the firmware download mode until either a succcessful firmware upgrade is completed or the power is cycled.

Step 16. Click **Transfer** > **Send File**. See *Figure B.9*.

Step 17. Specify the **Filename** to be the received firmware upgrade file.

Step 18. Specify the **Protocol** by selecting **1K Xmodem** from the drop-down menu.

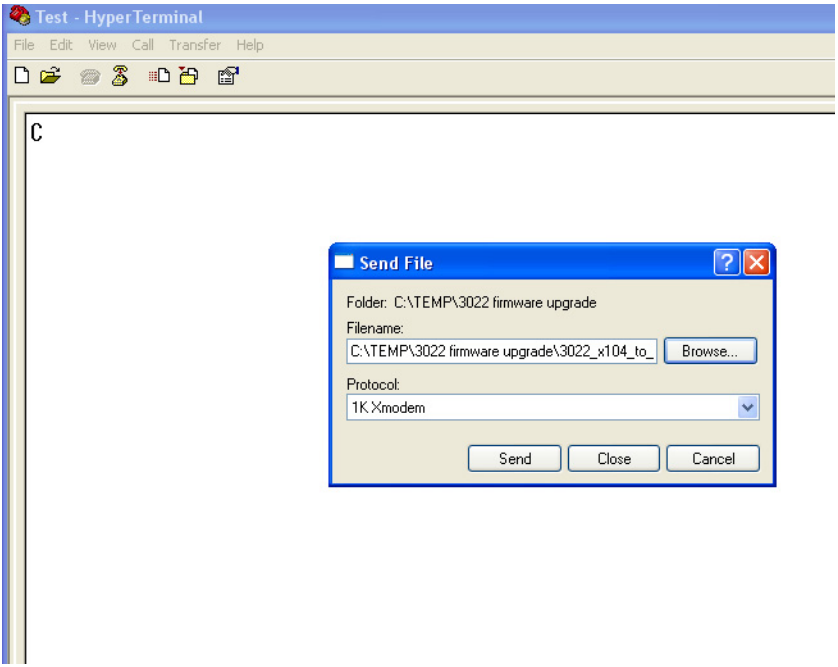

Figure B.9 Send File Prompt

Step 19. Click **Send**.

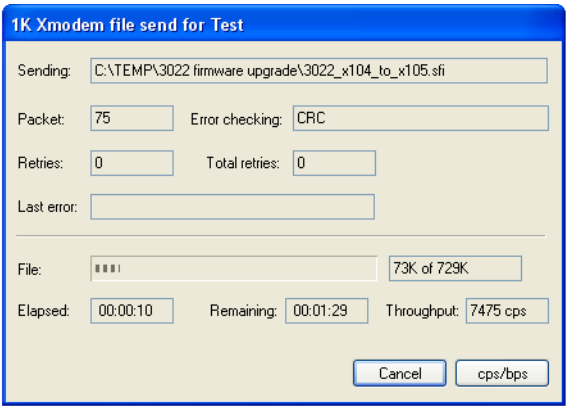

Figure B.10 Sending Confirmation Window

Step 20. If Xmodem transfer was successful, you will receive the validating firmware message. See first line of message in *Figure B.11*.

Step 21. If the firmware is invalid, you will receive an invalid firmware error message. See second line of message in *Figure B.11*.

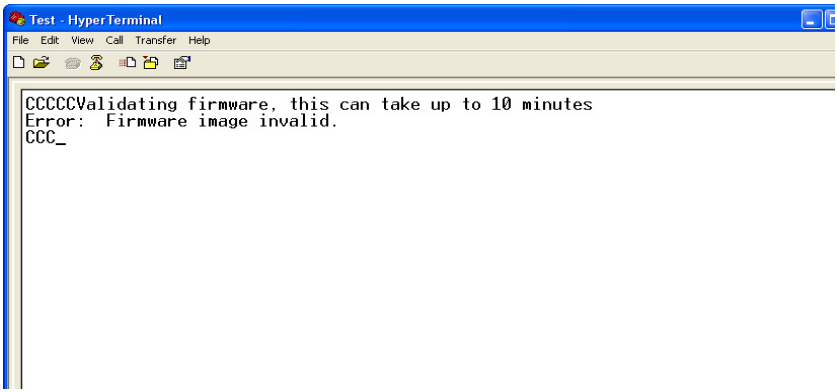

Figure B.11 Terminal Invalid Firmware Error Message

Step 22. Once the firmware is validated, you will receive the message that the firmware is being written to nonvolatile program memory (Flash).

IMPORTANT: Do not disconnect power during this stage.

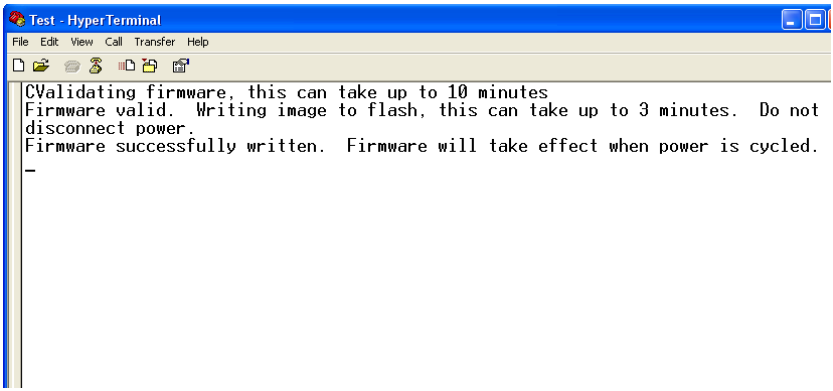

Figure B.12 Terminal Valid Firmware Message

Step 23. When successfully written to Flash, you will need to cycle power for the new firmware to take effect.

Step 24. After cycling power, you will need to reinitialize the SEL-3022 using the settings saved at the start of the firmware upgrade procedure.

Cryptographic Manual—Do Not Copy
Preliminary Copy

Factory Assistance

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 USA 99163-5603

Telephone: (509) 332-1890

Fax: (509) 332-7990

Internet: www.selinc.com

Preliminary Copy

Appendix C

Wireless Operator Interface Security

Introduction

The SEL-3022 incorporates a wireless LAN (WLAN) with which you can perform engineer access to IED and diagnostic and maintenance functions. The wireless aspect of the device makes connection of the SEL-3022 to a Personal Computer (PC) simple and efficient. Make such a connection through use of the SEL-5809 Settings Software or SEL-5810 Virtual Serial Software and 802.11b (also known as Wi-Fi) compliant devices standard with many new notebook PCs or available at most computer stores.

Preliminary Copy

Wireless Interface Security Overview

The SEL-3022 wireless operator interface and SEL-5809 Settings Software implement a two-part encryption system consisting of IEEE 802.11 WEP and the SEL Security Application. WEP is an encryption standard defined by the 802.11 specification and is available on most 802.11-enabled devices. The SEL Security Application consists of National Institute of Standards and Technology (NIST)-approved encryption and authentication algorithms that are cryptographically much stronger than WEP. Together, these two, independent security features provide a secure communications link between the SEL-3022 and the operator PC or Personal Data Assistant (PDA). Strengths of the WEP and SEL Security Application combination are as follows:

- A 104-bit WEP encryption function keeps out all but the most determined attackers. The following pages discuss the relative security of the WEP function.
- The SEL Security Application employs 128-bit AES encryption and 128-bit HMAC SHA-1 authentication. This application provides cryptographic security at greater than 128 bits of cryptographic key strength, using only FIPS 140-2 compliant cryptographic algorithms. The following pages discuss the SEL Security Application.

Figure C.1 shows the relationship between WEP and the SEL Security Application.

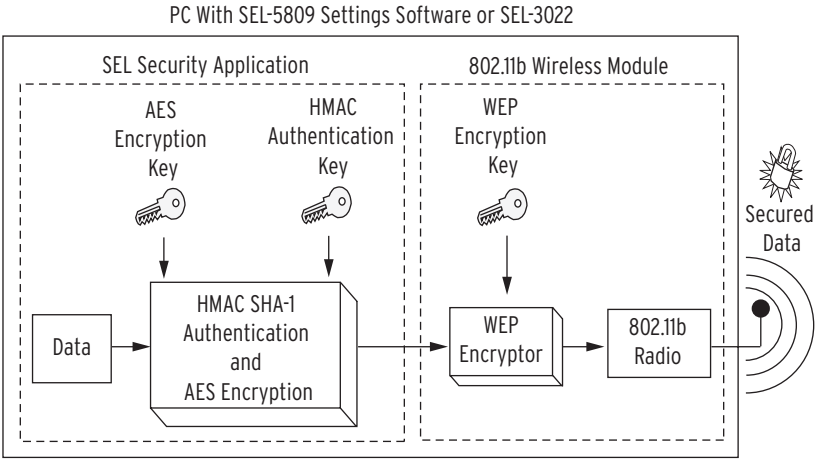

Figure C.1 Two Independent Layers of Cryptographic Security Protect the SEL-3022 Wireless Operator Interface

The decryption process of the SEL-3022 wireless interface consists of multiple cryptographic verifications. When the SEL-3022 wireless module receives a correctly addressed packet, the wireless module WEP decrypts the packet. The wireless module discards any packets that do not decrypt successfully. If the packets do WEP decrypt successfully, the wireless module passes resulting data frames to the SEL Security

Preliminary Copy

Application. The data frames must then AES decrypt and HMAC SHA-1 authenticate. If the SEL Security decryption or authentication fails, the SEL Security Application discards these data frames and disconnects. In summary, before the SEL-3022 considers data to be valid, the data must AES decrypt, HMAC SHA-1 authenticate, and WEP decrypt correctly, or the data are discarded. The process is reversed for the transmission and encryption process.

The SEL-3022/SEL-5809 Settings Software includes the following wireless security features:

- **104-Bit Wired Equivalent Privacy (WEP) Encryption:** The WEP encryption function, provided by the 802.11b wireless LAN module, is always enabled and active on the SEL-3022.
- **128-Bit Advanced Encryption Standard (AES) Encryption:** Because of the relative weakness of the WEP encryption function, the SEL-3022 also incorporates an independent layer of AES encryption.
- **128-Bit HMAC SHA-1 Frame Authentication:** Every frame transmitted on the wireless operator interface is cryptographically authenticated to prevent malicious tampering and to guarantee acceptance of only those frames that authorized users transmit.
- **Message Replay Protection:** The SEL-3022 uses frame sequence numbers with HMAC SHA-1 authentication to ensure that individual frames cannot be retransmitted to cause malicious actions.
- **Session Replay Protection:** The SEL-3022 uses a robust challenge-response session authentication protocol to guarantee that wireless operator sessions cannot be replayed to cause malicious actions.
- **AES and HMAC Session Key Exchange:** The SEL-3022 exchanges unique, randomly-generated encryption and authentication keys on each wireless session connection. This limits the amount of data protected by any single key value and strengthens the SEL-3022 against cryptanalytic attacks.
- **Wireless Session Password:** A configurable password is required to open a wireless connection with the SEL-3022. This password is never stored in the configuration software device image, so it cannot be compromised by theft of a configured maintenance PC containing the wireless encryption and authentication keys. In the event of a lost

Preliminary Copy

or stolen maintenance PC, this feature gives the system security officer time to change the cryptographic security parameters on the network.

- **Wireless Port Timeouts:** The SEL-3022 will not allow another wireless connection for a short period of time after any failed authentication attempt. This significantly reduces the rate at which a malicious individual can apply a brute force cryptographic key or password guessing attack.
- **Network Reconnaissance Protection:** The SEL-3022 will not reply to any network traffic that fails authentication. Because of this lack of response to unauthenticated network traffic, the SEL-3022 is not susceptible to ping sweeps and other network mapping techniques.
- **Single Active Session:** The SEL-3022 allows only a single active session and rejects attempts to establish a second wireless connection. This feature ensures that only one user can change settings at any given time.
- **No Default Settings:** The SEL-3022 will remain in an initialization mode when any of the critical security parameters are set to the default, zeroized values. During this initialization mode, the SEL-3022 will disable the wireless port and force the user to enter the initial encryption keys, authentication keys, and password values via a direct serial connection. This functionality ensures that critical security parameters are never transmitted over the 802.11b radio channel protected by insecure, factory default keys.

IEEE 802.11 WEP Security

The IEEE 802.11 designers included provisions for data encryption and authentication to provide what they considered strong data security and network access control. The Wired Equivalent Privacy (WEP) procedures outlined in the standard provide both functions. WEP encryption cryptographically scrambles the data contents of the Media Access Control (MAC) packet prior to transmission. The MAC packets can be intercepted, but the data scrambling the encryption process provides will, in theory, make the data payload and network headers (above the MAC network layer) incomprehensible. The encryption and decryption operations are a function of the original message data and a secret encryption key. For symmetric encryption algorithms, such as the RC-4 algorithm WEP uses, the encryption key and decryption keys are identical. Several factors, including the following, determine the strength or security of the encryption process:

- The secrecy of the key
- The length of the key
- How often the key value changes
- The cryptographic strength of the encryption algorithm

Because the encryption and decryption keys are identical for symmetric encryption algorithms, the theft or deduction of the key value by a malicious individual will remove any protection WEP encryption offers. There are a few common methods for determining a key value. The would-be attacker can simply steal the key value in some manner. If that option is not available, the attacker can attempt to guess the key value. The difficulty of such a guessing, or brute-force attack, grows exponentially with the length of the key. The encryption process can be strengthened against key-guessing attacks through periodic changes to the key value. If someone ever guesses the key value, the attacker can only decrypt the data processed with that key. Changing the key value on a periodic basis can significantly reduce the data a single key processes. Finally, the cryptographic strength of the encryption algorithm determines how difficult it is to compromise portions of the encrypted messages. If the algorithm is cryptographically sound, it is extremely difficult mathematically to compromise the key value or message contents from publicly available knowledge. Publicly available knowledge includes the encrypted message itself, known as ciphertext, and prior knowledge of the contents of the message This prior knowledge, for example, could include the statistics of English text or knowledge of the location and value of an encrypted header field. The IEEE 802.11 standard specifies that if the incoming packet cannot be decrypted properly, it must be dropped and ignored. All hosts must know the value of the secret encryption key prior to being granted network access. The network designer controls the dissemination of the key value and, therefore, controls who has access to the WEP-protected network.

WEP Security Flaws Explanation

WEP is based on a two-part encryption algorithm called RC-4. The first stage of the encryption process, known as the Key Scheduling Algorithm (KSA), takes a string of key bits as input and forms an output initialization string. The second stage, known as the Pseudo-Random Generation Algorithm (PRGA), produces a pseudo-random bitstream of arbitrary length. The value of this string of bits depends on the initializing permutation the KSA produces. Note that a given KSA input will always produce the same PRGA output. The designers of the IEEE 802.11 standard wanted the process of decrypting a single packet to be independent of all previous and future packets. Because of this requirement, the output of the PRGA function has to be reset at the beginning of every packet. If this were done without also changing the input to the KSA function, the encryption stream would be identical for every packet and the resulting encryption process would be trivially broken. Because of this, the input to the KSA function is a concatenation of a secret key (104 bits in the case of the SEL-3022 wireless operator interface) with a 24-bit Initialization Vector (IV). By changing the IV on every packet, the WEP encryption process ensures that the probability of any two, randomly chosen packets being encrypted with the same PRGA output (known as an "IV collision") is sufficiently low.

For each data packet, the concatenation of the key and IV serves as the input to the RC-4 algorithm, which produces a string of pseudo-random encryption bits (with a length equal to the length of the original data packet). To perform the encryption operation, the encryption bit string is added modulo 2 (XOR) to the original contents of the packet. The IV used during the encryption process is then concatenated with the resulting ciphertext to form the final message. A major contributor to the relative weaknesses of the WEP encryption process is the fact that the IV is appended to the ciphertext and transmitted unencrypted. The following text explains the details of these weaknesses.

In an August 2001 presentation at the Eighth Annual Workshop on Selected Areas in Cryptography of an article titled "Weaknesses in the Key Scheduling Algorithm of RC4," authors Fluhrer, Mantin, and Shamir published formal proofs of some potential weaknesses in the RC-4 algorithm. In a later paper, published in the AT&T Labs Technical Report TD-4ZCPZZ of August 2001 titled "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," authors Stubblefield, Ioannidis, and Rubin demonstrated that the WEP algorithm was designed in such a way as to contain the worst of the weaknesses that Fluhrer, Mantin, and Shamir's paper outlined. Furthermore, Stubblefield, Ioannidis, and Rubin demonstrated that a passive attack could be used to successfully determine a 104-bit secret key in just a few hours on a moderately loaded wireless LAN. Based on these results, Stubblefield, Ioannidis, and Rubin urged network designers to assume that the IEEE 802.11 link layer offers very little security and to employ additional security measures in addition to WEP. The SEL-3022 design incorporates these additional security measures in the form of cryptographically sound 128-bit AES encryption and HMAC SHA-1 authentication (see *The SEL Security Application on page C.9* for further explanation).

The weaknesses Fluhrer, Mantin, and Shamir described are a direct consequence of the RC-4 algorithm. These researchers demonstrated that there are large classes of keys for which a very small portion of the key determines a very large portion of the KSA output. Furthermore, Fluhrer, Mantin, and Shamir showed that the PRGA function is weak in the sense that known patterns in the KSA output are transformed into predictable patterns in the first byte of the PRGA output. In other words, for a large number of keys, the first byte of the PRGA output is highly correlated with a very small number of key bits. This correlation can be used, in certain situations, to guess the value of the secret key. The implementation of the WEP algorithm ensures that these weaknesses can be exploited in an effective manner. Because the WEP algorithm transmits the IV unencrypted with each packet, an attacker has full visibility of three bytes of the KSA input. Furthermore, the first encrypted byte of almost every IEEE 802.11 packet is a known constant. This is a direct consequence of the fact that the first encrypted byte of an IEEE 802.11 packet is the Destination Service Access Point (DSAP) field of the LLC header, which has a value of 0xAA (hexidecimal) for all packets containing TCP/IP protocol data. This known value allows an attacker to recover the first byte of the PRGA output for virtually every packet by simply XORing the first byte of ciphertext with the value 0xAA. Someone could attack WEP by observing the IV values of each encrypted packet transmitted on the network to find weak values that result in the leak of information about the value of a particular secret key byte into the first byte of the PRGA output. An attacker could repeat this process until all bytes of the secret key are determined with sufficiently high probability.

The 802.11b wireless LAN protocol provides a very effective wireless networking solution, which has resulted in steadily growing popularity of 802.11b-compliant networking devices, or access points (APs), since the introduction of the standard. This great popularity of such technology has fueled the development of software utilities designed to locate active wireless APs and identify whether WEP encryption is enabled on these devices.

If an attacker finds an AP protected by WEP encryption but interesting enough to warrant further investigation, the attacker can attempt to crack the WEP key. Several tools can passively capture normal wireless traffic on a target network and exploit the security flaws previously discussed to potentially determine the WEP encryption key used to secure the transmitted data. These tools have the potential to guess a WEP key by passively observing as few as four million network packets. Clearly, the time that this process takes is dependent on the average amount of network traffic that the 802.11 wireless network transmits.

Implications of WEP Security Flaws

Because of the previously discussed flaws, the WEP encryption function the 802.11 standard specifies does not provide the advertised 104 bits of cryptographic key strength. It does, however, provide a rather significant barrier to a potential attacker. It is difficult to determine the WEP key from a lightly loaded wireless network. A wireless connection between a maintenance PC and an SEL-3022 will only transmit network packets while the session is open and data are being actively exchanged between the PC and the SEL-3022. Under normal conditions, a potential attacker

would have to capture encrypted packets for an extremely long time to analyze the few million packets necessary to determine the WEP key and defeat the WEP encryption function. If an attacker successfully determines the WEP encryption key, the contents of all network packets transmitted between a maintenance PC and an SEL-3022 device would still be protected by the cryptographically strong encryption and authentication the SEL-3022 AES and HMAC SHA-1 functions provide (see *The SEL Security Application* section below for further explanation). The cryptographic community has scrutinized the AES encryption and HMAC SHA-1 authentication functions carefully, but cryptographers have been unable to find any security flaws similar to those contained in the WEP encryption function.

The SEL Security Application

The SEL Security Application consists of an authentication and encryption scheme that provides very strong data security. Authentication verifies message integrity (i.e., the message has not been altered). Encryption conceals the contents of the message. The combination of the two security techniques provides a state-of-the-art encryption and authentication system with a key strength greater than 128 bits. Proof of the security strength is detailed in the following sections.

HMAC SHA-1 Authentication Overview

The HMAC SHA-1 function provides protection against frame alteration and ensures (with extremely high probability) that the digital integrity of every frame remains intact. With a 128-bit-long authentication key, the HMAC SHA-1 function also provides strong frame authentication capability that allows confirmation that an authorized device transmitted the frame.

The National Institute of Standards and Technology (NIST) developed the SHA-1 one-way hash algorithm in 1993. NIST developed the Keyed-Hash Message Authentication Code (HMAC) algorithm in 2002. The SEL-3022 uses the proven SHA-1 one-way hash algorithm to form the NIST-approved HMAC SHA-1 keyed hash function.

The HMAC SHA-1 function takes a variable-length message and an authentication key as input and generates a 160-bit-long, fixed-length hash output value. The hash output is a condensed fingerprint or signature of the message input (see *Figure C.2*).

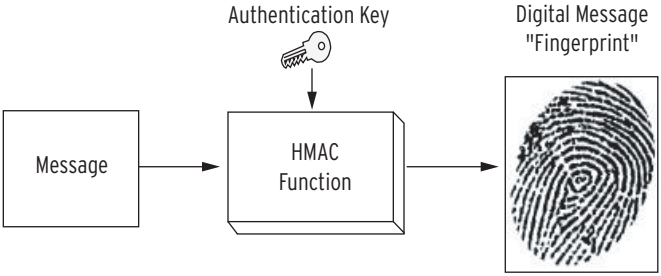

Figure C.2 Operation of the HMAC SHA-1 Keyed Hash Authentication Function

The 128-bit-long secret key gives the HMAC SHA-1 algorithm a strong built-in authentication capability. If an attacker changes the contents of the message, then the hash value appended to the message would not match the value that results from a newly calculated hash value over the new, altered message. Because the HMAC SHA-1 function is keyed (i.e., uses a secret authentication key to form the hash output), an attacker without knowledge of the authentication key value would be unable to recalculate a new, valid hash value over the altered message appended to the new message to hide the fact that the message has been altered.

To produce a cryptographically secure signature of a message, NIST designed the SHA-1 hash function to have the following properties:

- Given the SHA-1 hash function, *H(m)*, and its output, *h*, it is extremely difficult to derive a message, *m*, such that *H(m)* = *h*.
- Given a message, *m*, it is extremely difficult to find another message, *m*', that produces the same SHA-1 hash output.

The first condition states that the output of the SHA-1 hash function used in the HMAC authentication function does not give away any clues about the form, or classes, of messages that would likely produce the same hash value. The second condition, known as collision-resistance, states that there is no bias in the mapping of inputs to outputs that would aid an attacker in finding messages that produce identical SHA-1 hash values. Both conditions make it functionally impossible (given all realistic resources) to alter a message in such a way as to produce the same hash value. The HMAC specification provides a cryptographically secure way to combine the secret authentication key and the protected message into the SHA-1 hash function input to produce a key-dependent message fingerprint.

AES Overview

The AES encryption function uses a 128-bit-long secret key and scrambles the contents of each frame prior to transmission to provide cryptographically strong data confidentiality.

Encryption is the process of transforming a digital message from its original form into a form that an unauthorized individual cannot interpret. The output of the encryption process is a function of the message and an encryption key (see *Figure C.3*).

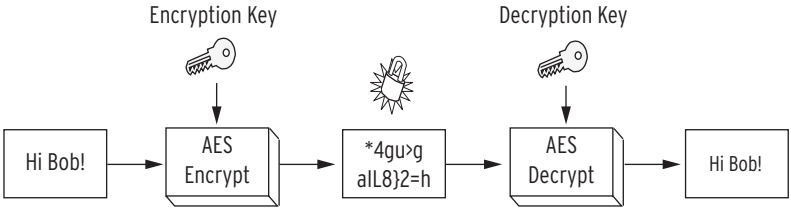

Figure C.3 Operation of the AES Encryption Function

This encryption process must be completely reversible by an authorized individual with access to the secret decryption key. Authority to read a message is only granted by sharing knowledge of the secret decryption key. Ideally, only individuals with knowledge of the decryption key can reverse the encryption operation and interpret the protected message. There are two main classes of encryption functions. Symmetric key encryption relies on the same secret key value, K, to perform both the encryption and decryption transformations. Asymmetric key encryption, on the other hand, uses a different key for encryption and decryption. For example, asymmetric encryption

might use K1 for encryption and K2 for decryption. The AES encryption algorithm the SEL-3022 uses is a symmetric block cipher, with an encryption/decryption key size of 128 bits.

The Advanced Encryption Standard (AES) is the latest encryption standard adopted by the National Institute of Standards and Technology (NIST). In 1997, NIST challenged the cryptographic community to develop the next generation encryption algorithm to replace the aging DES and 3DES encryption standards. In 2000, NIST chose the Rijndael encryption algorithm as the AES encryption standard. During the evaluation of candidates for the AES standard, some of the best cryptanalysts in the world analyzed and approved Rijndael. Since NIST adopted the standard in 2001, AES has proven to be very effective against known attacks.

Combined HMAC SHA-1 and AES Encryption Security

Every frame transmitted over the SEL-3022 wireless operator interface is authenticated with an HMAC SHA-1 keyed hash digest and encrypted with the AES encryption algorithm (both algorithms are described in detail in the *HMAC SHA-1 Authentication Overview* and *AES Overview* sections above). As shown in *Figure C.4*, the SEL-3022 first forms the HMAC SHA-1 hash output from the original frame data payload and the 128-bit authentication key. This keyed message fingerprint is then appended to the end of the frame data payload, and the resulting composite message is encrypted by the AES encryption function through use of a separate, 128-bit encryption key (the authentication key and encryption key are completely independent).

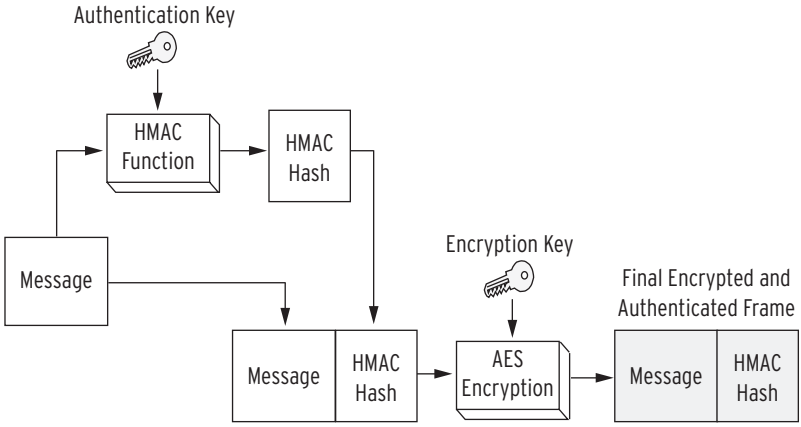

Figure C.4 SEL-3022 Security Application Overview

Upon receipt of any frame on the wireless operator interface, the SEL-3022 uses the programmed 128-bit secret encryption/decryption key to AES decrypt the entire frame. The SEL-3022 then uses the programmed 128-bit authentication key to calculate the

HMAC SHA-1 keyed hash value over the payload (message) portion of the received frame. If the calculated HMAC SHA-1 hash output does not match the received message fingerprint, the SEL-3022 rejects the message and terminates the session.

This arrangement protects the original frame data payload from malicious alteration, authenticates the origin of the frame as a device with knowledge of both the encryption and authentication keys, and protects the contents of the frame data payload from theft.

SEL Security Application Analysis

Cryptographic experts have analyzed the AES and HMAC SHA-1 cryptographic functions. This analysis process began before NIST accepted each of the functions as standards, and it will continue as long as these standards remain in use. To date, the AES encryption and HMAC SHA-1 authentication algorithms have withstood all public scrutiny in the sense that they provide the advertised level of security. In other words, an AES encryption function with a 128-bit key will, by all analysis to date, provide data confidentiality at a cryptographic strength of 128 bits (the discussion in the following text addresses this concept). Cryptographically sound hash functions, such as SHA-1, are expected to provide message integrity functionality at a strength equal to half the size of the hash output. Because SHA-1 has a hash output length of 160 bits, it should produce message integrity functionality at a cryptographic strength of 80 bits. To date, SHA-1 has maintained the expected cryptographic strength. Finally, the HMAC function has also withstood all cryptographic analysis, in the sense that it has proven to be an effective and secure method of mixing a secret authentication key into the SHA-1 hash output. We will analyze the implications of these statements in the following text.

As stated previously, the AES encryption function has, thus far, provided data confidentiality at a cryptographic strength equal to the size of the encryption key. To successfully guess a 128-bit key, such as the key the SEL-3022 uses, an attacker would have to try an average of $2^{127} = 1.7 \cdot 10^{38}$ keys before finding the correct value (assuming that all key values are equally likely). This is a staggering number of potential key values! If an attacker could test one million potential keys per second, it would take more than $5.39 \cdot 10^{24}$ years, on average, to guess the correct key value (note that the universe is estimated to be only 10^{13} years old)! In reality, the time that it would take to launch an effective key guessing attack against the SEL-3022 would be even longer, because the wireless interface on the SEL-3022 times out briefly when an authentication failure occurs. Because of the wireless interface timeout, the maximum rate of a key guessing attack against the SEL-3022 is much less than one million keys per second.

Because the SEL Security Application AES encrypts the HMAC-keyed authentication digest in every frame, both the AES encryption key and the HMAC SHA-1 authentication key must be compromised simultaneously to send data to the SEL-3022. For such a situation, an attacker would have to guess two independent 128-bit key values, which is the same as guessing a single, 256-bit key. To guess a key of this size, an attacker would, on average, have to make $2^{255} = 5.79 \cdot 10^{76}$ key guessing attempts. If an attacker could test one million potential keys per second, it would take more than

$1.83 \cdot 10^{63}$ years, on average, to guess both the authentication key and the encryption key values. The analysis just described suggests that it is statistically impossible to launch a key guessing attack against the SEL-3022 device that would result in compromise of the system.

Even if someone were to steal a maintenance PC with the wireless interface encryption and authentication keys programmed and saved on the PC hard drive, an attacker would have to crack the SEL-3022 connection password to use the stolen computer to successfully authenticate with the SEL-3022. To launch a password guessing attack, an attacker would have to repeatedly send an initial session request frame and enter the password guess into the SEL-5809 Settings Software dialog box.

If the entered password value is incorrect, the SEL-3022 terminates the session authentication dialog after receiving Frame 3 of the authentication dialog (see *Figure C.5 on page C.15* and the discussion *Connection Authentication and Session Replay Protection on page C.14*). If the authentication dialog fails at any point, the SEL-3022 performs a timeout of the wireless operator interface and refuses any session connection requests for five seconds. This limits the rate of a password guessing attack to one guess per five seconds.

The SEL-3022 accepts password entries between 6 and 80 characters in length. These passwords can contain all 96 printable ASCII characters (including the Space character). If we assume that the security officer has programmed strong passwords into the SEL-3022, an attacker would not be able to use a typical password guessing attack dictionary to limit the number of required password guesses. In this case, all possible password values would be equally likely and the attacker would have to launch a brute-force password guessing attack by sending all possible password values to the SEL-3022, one at a time. *Table C.1* shows the number of potential password values (i.e., the maximum number of guesses that an attacker will have to make) and the average number of years required to launch a successful brute-force password guessing attack on the SEL-3022 as a function of the length of your programmed password value. The value representing the average number of years required to successfully guess the SEL-3022 connection password was derived under the assumption that all potential password values are equally probable (i.e., you do not program a password value that is likely to be in an attack dictionary). Such strong passwords do not form a word, slang term, or other meaningful value. A strong password also contains a mixture of alphanumeric characters (numbers and uppercase and lowercase letters) and non-alphanumeric characters (punctuation characters, backslash, space, etc.).

Table C.1 Number of Years Required to Guess an SEL-3022 Password

Password Length	Number of Possible Password Values	Average Number of Years Required to Guess the Password (Assuming Strong Password Choice)
6	$7.91 \cdot 10^{11}$	$6.27 \cdot 10^{4}$
7	$7.59 \cdot 10^{13}$	$6.02 \cdot 10^{6}$
8	$7.29 \cdot 10^{15}$	$5.78 \cdot 10^{8}$

Table C.1 Number of Years Required to Guess an SEL-3022 Password

Password Length	Number of Possible Password Values	Average Number of Years Required to Guess the Password (Assuming Strong Password Choice)
...	...	...
80	$3.86 \cdot 10^{158}$	$3.06 \cdot 10^{151}$

Even with a strong, six-character password, an attacker could expect to spend more than 60,000 years trying to launch a successful brute-force password-guessing attack on the SEL-3022. Such a brute-force password guessing attack is statistically impossible because of the potential strength of the SEL-3022 connection passwords (very long password length with the password consisting of a very large number of possible characters), and password-guessing rate limit that the five-second wireless port timeout imposes on all connection authentication failures.

Connection Authentication and Session Replay Protection

SEL-3022 Wireless Port Status Prior to Security Parameter Initialization

The SEL-3022 uses two access levels for monitoring and configuration. Each access level has the following security parameters: 128-bit encryption key, 128-bit authentication key, and a password containing as many as 80 characters. Also included in the security parameters are the 104-bit WEP keys. From the factory, cryptographic security parameters are zeroized. At power up, the SEL-3022 determines if the cryptographic security parameters are set to trivial (zero) values. If these parameters are set to trivial values, the 802.11b wireless port is disabled. If the SEL-3022 is initialized with zeroized values, or if any of these initial security parameters are left at a zeroized value, the device will not leave the initialization mode, and the wireless port will remain disabled. Following entry of non-zeroized security parameters, the SEL-3022 enables the wireless module and enables both WEP and the SEL Security Application. This ensures that data are never transmitted via the 802.11b interface with default/trivial encryption keys.

SEL-3022 Security Parameters and Passwords

The SEL-5809 Settings Software is necessary to initiate a wireless session. The SEL-5809 Settings Software must be programmed with identical encryption and authentication security parameters as the SEL-3022 to which it will be connected. Furthermore, you must enter into the SEL-5809, when prompted, the same password stored in the SEL-3022. Note that neither a PC nor a PDA stores this password; the user must enter this password from memory. Because the PC does not store password values, no one can use just a PC or PDA to connect successfully with the SEL-3022

without direct knowledge of the correct password value. This remains true even if someone attempts a connection through use of a stolen PC with the correct wireless authentication and encryption keys programmed into the device image.

SEL-3022/SEL-5809 Wireless Interface Session Authentication Dialog

To begin a wireless operator interface session, the PC or PDA must authenticate with the SEL-3022 to prove that it has been programmed with the exact values of the expected authentication key and encryption key, and that you entered the correct password. *Figure C.5* provides an overview of the session authentication dialog between a maintenance PC with the SEL-5809 Settings Software installed and an SEL-3022 device. Each frame of this five-frame dialog is protected by the encryption and authentication methods described previously. Because of these protection methods, the data in each frame are secured by strong AES encryption and the SEL-5809 Settings Software, and the SEL-3022 can verify that an authorized device (i.e., a device with direct knowledge of the encryption key and authentication key values) sent every frame.

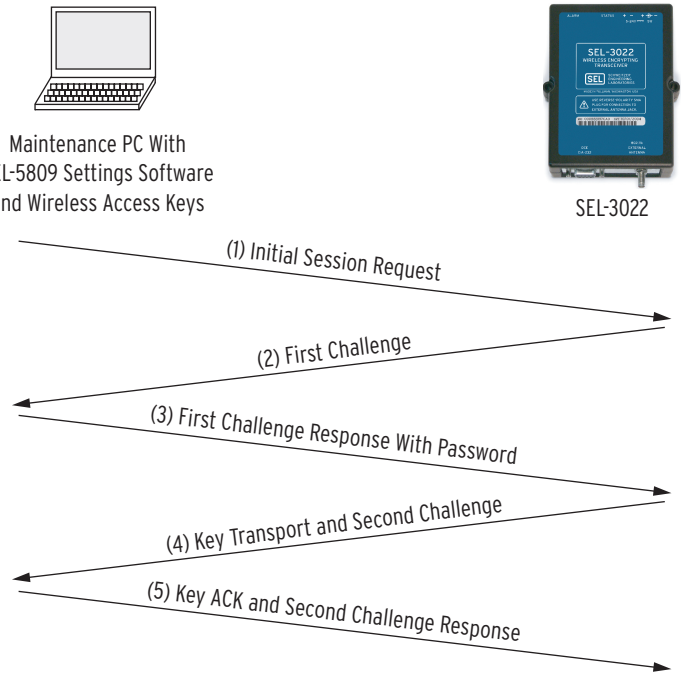

Figure C.5 Wireless Interface Session Authentication Dialog

The connection dialog begins with a connection request frame (Frame 1 in *Figure C.5*) that is encrypted and authenticated with encryption and authentication keys programmed into the SEL-5809 Settings Software device image. Upon receiving the connection request, the SEL-3022 decrypts and authenticates the frame. If the authentication fails, indicating that the session request came from other than an authorized user (i.e., a PC programmed with the appropriate AES encryption and HMAC SHA-1 authentication keys), the SEL-3022 ignores the session request and remains silent. Note that the initial connection frame must be directed at the correct User Datagram Protocol (UDP) port on the wireless TCP/IP interface of the SEL-3022 transceiver. Because the UDP protocol does not require a connection handshake, as does TCP protocol, the SEL-3022 only transmits a TCP/IP frame in response to a fully authenticated connection request frame. This feature ensures that the SEL-3022 is immune to traditional port mapping and network reconnaissance techniques such as ping sweeps, TCP SYN scans, or TCP FIN scans.

If the initial connection request frame passes the authentication process, the SEL-3022 generates a large, random challenge value and transmits it to the PC (Frame 2 in *Figure C.5*). Upon receipt of the First Challenge frame, the PC must insert the received challenge value into a new encrypted and authenticated frame and transmit it to the SEL-3022 (Frame 3 in *Figure C.5*). In addition, this First Challenge frame contains the password information you entered in the SEL-5809 Settings Software session connection dialog box. When the SEL-3022 receives this frame, it decrypts and authenticates it. If the authentication fails, again indicating that the session request came from an unauthorized user, the SEL-3022 terminates the session and resets the session connection dialog. If the frame passes authentication, the SEL-3022 compares the transmitted password information with the password value stored in the SEL-3022 settings. It is important to note that if the transmitted password information indicates that the user entered the wrong password, or if the decrypted challenge value does not match the challenge value transmitted in Frame 2 of the connection dialog, the SEL-3022 again terminates the session and resets the connection dialog.

- The password you entered in the SEL-5809 Settings Software must match the password value stored in the SEL-3022 device, or the session connection will fail. This guarantees that a stolen maintenance PC programmed with the correct encryption and authentication keys cannot be used to connect to the SEL-3022 without the user having direct knowledge of the programmed password value stored in the SEL-3022 (the SEL-5809 Settings Software never stores the password value on the PC hard drive).
- The large, random challenge value that the SEL-3022 formed and transmitted in Frame 2 of the connection dialog is, with very high probability, different for every wireless session. Because of this large, random value, a malicious individual cannot capture a previous session dialog and use the captured packets to reconnect to the SEL-3022 (known as a **session replay** attack). If someone attempted such an attack, the challenge value transmitted in the First Challenge Response With Password frame (Frame 3 in *Figure C.5*) would not

match the challenge value the SEL-3022 issued in the First Challenge frame (Frame 2 in *Figure C.5*), and the SEL-3022 would terminate the connection attempt.

If the connection dialog succeeds up to this point (i.e., passes all authentication mechanisms and session replay protection mechanisms described previously), the SEL-3022 generates another random challenge value, a random session encryption key, and a random session authentication key and transmits these values in Frame 4 of the session connection dialog. The SEL-3022 uses these session keys, protected from interception by SEL Security Application cryptographic mechanisms, described in the previous sections, to encrypt and authenticate all configuration frames transmitted between the PC and the SEL-3022 after the five-frame session authentication dialog succeeds.

Upon receiving the Key Transport and Second Challenge frame, the PC must insert the transmitted second challenge value into the final frame of the session connection dialog (Frame 5 in *Figure C.5*) and transmit the frame to the SEL-3022. To complete the session authentication dialog successfully, the decrypted and authenticated challenge value the SEL-3022 received in Frame 5 must match the value the SEL-3022 transmits in Frame 4. This requirement for matching values forms a second, independent layer of protection against session replay attacks.

If the final frame authenticates correctly and the second challenge values match, the SEL-3022 opens a wireless operator interface connection with the PC. All configuration frames transmitted between the two devices after successful completion of the session authentication dialog previously described will be encrypted and authenticated through use of the session encryption and authentication keys exchanged in the dialog.

The SEL-3022 connection authentication provides strong security against a number of potential threats. We summarize the security features of this connection authentication dialog as follows:

- There are two, independent challenge/response exchanges to prevent session replay attacks.
- There is strong protection against threats posed by maintenance PC theft. The user must enter from memory, the correct connection password to successfully authenticate to the SEL-3022 (the connection password is never stored on the maintenance PC).
- Unique session encryption and session authentication key exchanges limit the number of frames protected by the programmed operator and security officer role encryption and authentication keys. This makes the SEL-3022 more resilient to cryptanalytic attacks.

Frame Replay Protection

Every frame in a given wireless operator interface session contains a sequence number field. The value in this field increments every time a frame is transmitted over the interface. The SEL-3022 will not accept any frame that contains a sequence number

value that is less than, or equal to, the sequence number value received in the last frame. It is exceedingly difficult to maliciously alter the sequence number in any given frame to bypass this functionality because the sequence number field is protected by the strong cryptographic authentication mechanisms provided by the HMAC SHA-1 function. Because of the protection these mechanisms provide, an attacker cannot capture a frame, previously transmitted in a given wireless operator interface session, and resend the frame to the SEL-3022 to cause harmful actions.

Conclusions

Two independent layers of cryptographic security protect the SEL-3022 wireless operator interface: the 802.11b wireless interface module WEP encryption function, and the AES encryption and HMAC SHA-1 authentication functions in the SEL Security Application. For an attacker to compromise the SEL-3022 operator interface, both the WEP encryption and the SEL Security Application have to be defeated. As shown in the discussion above, the probability of an attacker accomplishing this is statistically impossible.

Additional Protection for Windows XP Users

IMPORTANT: Windows XP users can further protect their computer during setup by enabling a firewall on their wireless connection. This firewall protects your computer from unauthorized users who might try an ad hoc connection. This will not impact your ability to configure the SEL-3022.

Follow these steps to enable a firewall on Windows XP Wireless Connection.

Step 1. Click on the **Start** menu, select **Settings**, then **Network Connections**, and then **Wireless Connection**.

Step 2. Click on the Wireless connection you used to communicate with the SEL-3022 (example: **Wireless Connection 2**).

Step 3. Click on **Properties**, then the **Advanced** tab.

Step 4. Click on the box beside **Protect my computer and network by limiting or preventing access to this computer from the Internet**.

Step 5. Click **OK**.

Preliminary Copy

Appendix D
Certificates

ISO

The device is designed and manufactured through use of an ISO 9001 certified quality program.

Listings

IEC 60950-1: 1st Ed./CSA C22.2 No. 60950-1/EN 60950-1

FCC

15.247

IC

ICES-001

Preliminary Copy

This page intentionally left blank

Preliminary Copy

Glossary

AES

Advanced Encryption Standard - sponsored by NIST, AES was developed for securing sensitive but unclassified material by U.S. Government agencies. AES is a symmetric encryption algorithm (same key for encryption and decryption) that uses block encryption.

FIPS 140-2

Federal Information Processing Standards 140-2 specifies the security requirements satisfied by a cryptographic module in use within a security system that protects sensitive but unclassified information. The standard provides four increasing, qualitative levels of security. The security requirements cover areas related to the secure design and implementation of a cryptographic module.

IED

Intelligent Electronic Device. An IED, as defined in this document, is a device capable of receiving information and sending appropriate responses. Examples of IEDs are remote terminal units, programmable logic controllers, communication processors, relays, meters, etc.

NIST

National Institute of Standards and Technology, a unit of the U.S. Commerce Department.

WEP

Wired Equivalent Privacy is a security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11b. WEP is designed to provide a wireless local area network (LAN) with a level of security and privacy comparable to that associated with a wired LAN.

Preliminary Copy

This page intentionally left blank

Preliminary Copy

Preliminary Copy

Solutions

Systems, Services, and Products for the Protection, Monitoring, Control, Automation, and Metering of Utility and Industrial Electric Power Systems Worldwide.

Attention

The SEL-3022 is a cryptographic device. Limit access to the SEL-3022, SEL-5809 Settings Software, SEL-5810 Virtual Serial Software, and SEL-3022 Instruction Manual to authorized personnel only. Do not copy these items. Securely store these items when not in use. Destroy these items when no longer needed.

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: 509.332.1890 • Fax: 509.332.7990
www.selinc.com • info@selinc.com