

FIRE

SafeLINC™ Fire Panel Internet Interface (FPII)



Installation, Setup
& Operating
Instructions

579-349
Rev. H

Copyright and Trademarks

Copyright

© 2002-2011 SimplexGrinnell LP. All rights reserved

Specifications and other information shown were current as of publication and are subject to change without notice.

Trademarks

SafeLINC, TrueAlarm, Simplex, and the Simplex logo are trademarks of Tyco International Ltd. and its affiliates and are used under license.

Microsoft is a registered trademark of Microsoft Corporation.

Windows is a trademark of the Microsoft Corporation.

All other logos and product names are trademarks or registered trademarks of their respective companies.

Cautions and Warnings

Cautions and Warnings



READ AND SAVE THESE INSTRUCTIONS. Follow the instructions in this installation manual. These instructions must be followed to avoid damage to this product and associated equipment. Product operation and reliability depend upon proper installation.

DO NOT INSTALL ANY SIMPLEX® PRODUCT THAT APPEARS DAMAGED- Upon unpacking your Simplex product, inspect the contents of the carton for shipping damage. If damage is apparent, immediately file a claim with the carrier and notify an authorized Simplex product supplier.



ELECTRICAL HAZARD - Disconnect electrical field power when making any internal adjustments or repairs. All repairs should be performed by a representative or authorized agent of your local Simplex product supplier.



EYE SAFETY HAZARD – Under certain fiber optic conditions, the optical output of this device may exceed eye safety limits. Do not use magnification (such as a microscope or other focusing equipment) when viewing the output of this device.



STATIC HAZARD - Static electricity can damage components. Handle as follows:

- Ground yourself before opening or installing components.
- Prior to installation, keep components wrapped in anti-static material at all times.

Service Requirements

In the event of equipment malfunction, a representative of your local Simplex product supplier should perform all repairs. It is the responsibility of users requiring service to report the need for service to your local Simplex product supplier.

Contents

Introduction to the SafeLINC FPII	1
Introduction.....	1
Overview.....	1
Requirements	2
SafeLINC FPII Card Illustration.....	2
SafeLINC FPII Card Specifications.....	3
General Temperature/Humidity Requirements	3
Specific Temperature/Humidity Requirements.....	3
Power Requirements	3
Configuring the SafeLINC FPII Card.....	4
Overview.....	4
Setting Communications	4
Setting Computer Port Protocol (CPP) Functionality	4
Setting the Baud Rate and Address.....	5
Mounting the SafeLINC FPII Card.....	7
Overview.....	7
4100U/4100ES Mounting	7
4010ES Mounting	8
4100/4120 Mounting.....	9
4020 Mounting.....	10
SafeLINC FPII Field Wiring.....	11
Overview.....	11
4100U/4100ES/ 4010ES-Style Wiring	11
4100/4120 Legacy Wiring	12
4020-Style Wiring.....	13
LED Indicators.....	14
Interpreting LED Indications	14
Adding the SafeLINC FPII to the FACP via the Programmer.....	16
Overview.....	16
Using the DOS-Based Programmer	16
Using the Windows-Based Programmer.....	21
Connecting a PC to the SafeLINC FPII Diagnostic & Configuration Port....	26
Connecting SafeLINC FPII Card to a PC	26
Configuring a Terminal Emulation Program	26
Checking for Duplicate IP Addresses	26
Using the Boot Menu	28
Completing the MIS/IT Configuration Worksheet	28
Entering Data from the MIS/IT Configuration Worksheet	29
Starting Up the SafeLINC FPII.....	31
Logging In as an Administrator	31
The Home Page.....	32
Overview.....	32
The Home Page.....	32
The Administration Menu.....	32
Login Accounts.....	33
Overview.....	33
Setting Up a New User Account	33
Adding/Editing a User Account.....	33
Changing the Administrator Password.....	34
Email Configuration.....	35
Overview.....	35
Configuring SafeLINC FPII Email	35
Disabling Outgoing Email	36
Configuring the Email Health Status Check	36
Customizing Event Messages	36
Understanding Email Event Notification	37

Security Settings	38
Overview	38
Description of Security Settings	38
Customize Links	40
Setting Up the Home and User Links Pages	40
Updating Firmware	41
Overview	41
Firmware Update Procedure	41
Summary	43
Viewing a Summary of Administrative Changes	43
General Operations	44
The System Menu	44
Checking the System Status	44
Viewing System, Card, and Point Reports	46
Overview	46
Viewing TrueAlarm Service Reports	46
Viewing TrueAlarm Status Reports	46
Viewing Point Summaries	46
Viewing Card Summaries	47
Viewing the SafeLINC FPII/Host Panel Summary	47
Viewing Alarm and Trouble Logs	47
Basic Reports	48
Overview	48
Report Items	48
MIS/IT Configuration Worksheet	49

Introduction to the SafeLINC FPII

Introduction

This document can be used with FPII installed on the 4100ES, 4100U, 4100, 4010ES, 4120, and 4020-Series Fire Alarm Systems. Table 1 lists SafeLINC FPII Product ID numbers (PIDs) and the compatible Fire Alarm Control Panel (FACP) PIDs.

Table 1. SafeLINC FPII & Compatible FACP PIDs

SafeLINC FPII Product ID	Compatible FACP Product ID
4100-6060	Any 4100U/4100ES FACP Product ID
4010-9913	Any 4010ES FACP Product ID
4120-0160	4120-8001, -8010, -8201, -8210, -8511, -8601, -8700, -8701, & -8721
4100-0160	4100-8001, -8010, -8201, -8210, -8511, -8601, & -8701
4020-0160	4020-8001

Overview

The Fire Panel Internet Interface (SafeLINC FPII) is a module that interfaces to a 4100ES, 4100U, 4100, 4010ES, 4120, or 4020 Fire Alarm Control Panel (FACP), and it provides the following:

- Ability to access FACP data using the Internet Explorer (IE) 5.0+ web browser in conjunction with a Win98, ME, NT, or 2000 operating system.
- Ability to send email messages for prioritized event notification and scheduled email of Dirty/Excessively Dirty detector status information. (The SafeLINC FPII functions as an information kiosk that's accessible via the Internet rather than as a remote annunciator.)
- Ability to email reports for TrueAlarm[®] Sensor Status, TrueAlarm Sensor Service, and historical logs (fire alarm, Priority 2 alarm, trouble, and supervisory) on demand or via a schedule (weekly, bi-weekly, or monthly).

This publication describes how to:

- Install the SafeLINC FPII card.
- Configure the SafeLINC FPII for operation on your local network.
- Configure the SafeLINC FPII Administrative Account.
- Configure the SafeLINC FPII to send email.
- Use the SafeLINC FPII.

Notes:

- It is strongly recommended that both your operating system and web browser contain the latest patch updates.
- The SafeLINC FPII is for ancillary use only and does not provide any fire alarm or burglary function other than reporting of system status.

Introduction to the SafeLINC FPII, *Continued*

Requirements

To use the SafeLINC FPII properly, you must meet the following requirements:

- Win98, ME, NT, or 2000 Operating System
- Internet Explorer (IE) 5.0+ web browser
- FACP System Firmware: V9.02.02, 10.61, 11.03, or greater
- 4100ES, 4100U, 4100, 4010ES, 4120, or 4020 FACP

SafeLINC FPII Card Illustration

Figure 1 depicts the SafeLINC FPII card.

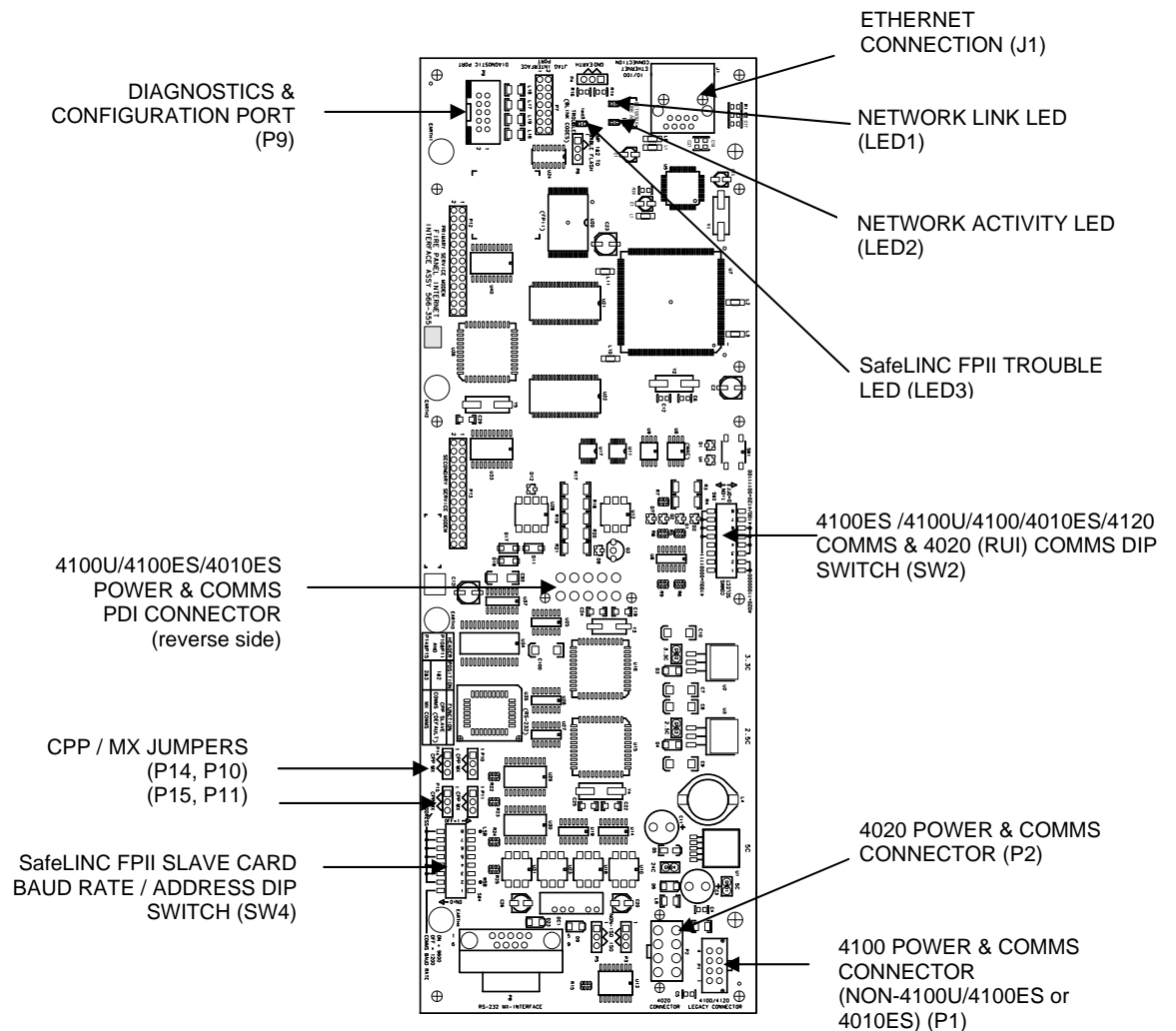


Figure 1. The SafeLINC FPII Card

SafeLINC FPII Card Specifications

**General
Temperature/Humidity
Requirements**

The following general temperature/humidity specifications apply to the SafeLINC FPII card.

The equipment operates normally with ambient temperatures outside the cabinet from 32° to 120° F (0° to 49° C), inclusive.

The equipment operates normally under non-condensing humidity conditions up to 93% relative humidity at 90° F (32° C).

**Specific
Temperature/Humidity
Requirements**

Effective Operating Temperature Range 32° to 120° F (0° C to 49° C), assuming 41° F (5° C) rise in FACP cabinet.

Effective Operating Humidity Range 10 to 93% relative humidity ($\pm 2\%$)
non-condensing at 90° F (32° C) ($\pm 2^\circ$).

Power Requirements

SafeLINC FPII power is supplied from system FACP 24 V. On-board power supplies include 5 V, 3.3 V, and 2.5 V with each supply powered from the 24 V FACP connection.

Maximum Battery Standby Current Draw 115 mA Maximum on 24 V rail (Worst Case).

Configuring the SafeLINC FPII Card

Overview

This section describes how to configure the SafeLINC FPII card using DIP switches and jumpers.

Setting Communications

DIP switch SW2 is used to set the SafeLINC FPII card's communications to either 4020/RUI-Style, 4100/4120 Legacy, or 4100U/4100ES/4010ES-Style communications. Set the DIP switch according to the illustration.

IMPORTANT: For proper communications, recheck the SW2 settings before applying power.

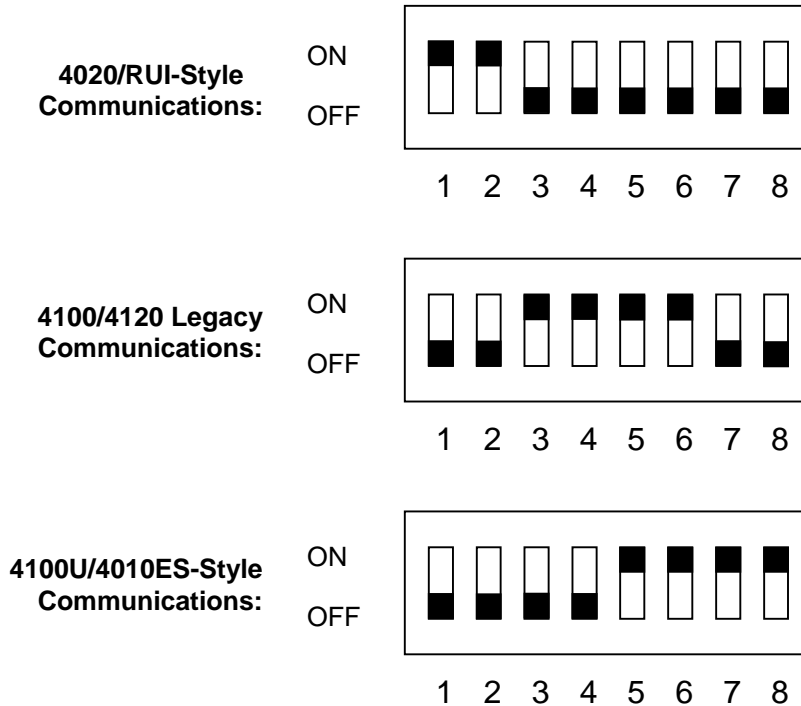
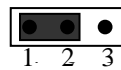


Figure 2. SW2 Switch Settings

Setting Computer Port Protocol (CPP) Functionality

Use **P10**, **P11**, **P14** and **P15** to set the SafeLINC FPII card's incoming protocol. Verify that **P10**, **P11**, **P14** and **P15** are all set to Positions 1 and 2. You should not have to change the positions because they are set to Positions 1 and 2 by default from the factory.



P10, P11, P14, P15: Positions 1-2: CPP (default from factory).
Positions 2-3: Reserved for future use.

Configuring the SafeLINC FPII Card, *Continued*

Setting the Baud Rate and Address

The device address is set via DIP Switch SW4, which is a bank of eight switches. From left to right (see Figure 3 below), these switches are designated as SW4-1 through SW4-8. The function of these switches is as follows:

- **SW4-1.** This switch sets the baud rate for the internal communications line running between the card and the FACP CPU. Set this switch to ON for 9600 baud communication.
- **SW4-2 through SW4-8.** These switches set the card's address within the FACP. Refer to Table 2 for a complete list of the switch settings for all of the possible card addresses.

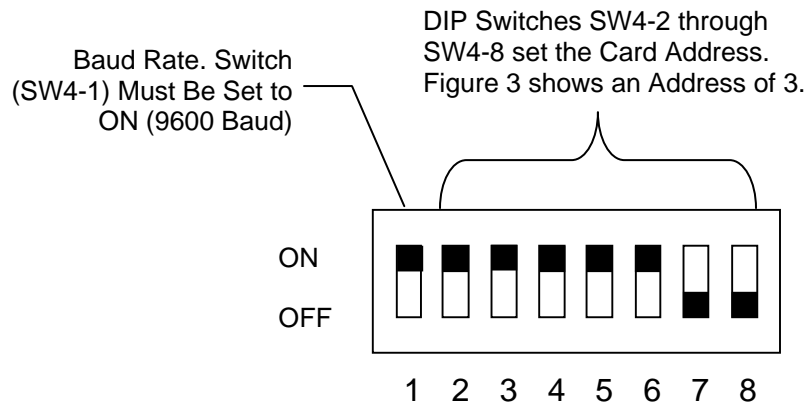


Figure 3. SW4 Switch Settings

Continued on next page

Configuring the SafeLINC FPII Card, *Continued*

Setting the Baud Rate and Address

Table 2. Card Addresses

Address	SW 1-2	SW 1-3	SW 1-4	SW 1-5	SW 1-6	SW 1-7	SW 1-8	Address	SW 1-2	SW 1-3	SW 1-4	SW 1-5	SW 1-6	SW 1-7	SW 1-8
1	ON	ON	ON	ON	ON	ON	OFF	61	ON	OFF	OFF	OFF	OFF	ON	OFF
2	ON	ON	ON	ON	ON	ON	OFF	62	ON	OFF	OFF	OFF	OFF	OFF	ON
3	ON	ON	ON	ON	ON	ON	OFF	63	ON	OFF	OFF	OFF	OFF	OFF	OFF
4	ON	ON	ON	ON	ON	OFF	ON	64	OFF	ON	ON	ON	ON	ON	ON
5	ON	ON	ON	ON	ON	OFF	ON	65	OFF	ON	ON	ON	ON	ON	OFF
6	ON	ON	ON	ON	ON	OFF	OFF	66	OFF	ON	ON	ON	ON	OFF	ON
7	ON	ON	ON	ON	ON	OFF	OFF	67	OFF	ON	ON	ON	ON	OFF	OFF
8	ON	ON	ON	ON	OFF	ON	ON	68	OFF	ON	ON	ON	OFF	ON	ON
9	ON	ON	ON	ON	OFF	ON	ON	69	OFF	ON	ON	ON	OFF	ON	OFF
10	ON	ON	ON	ON	OFF	ON	OFF	70	OFF	ON	ON	ON	OFF	OFF	ON
11	ON	ON	ON	ON	OFF	ON	OFF	71	OFF	ON	ON	ON	OFF	OFF	OFF
12	ON	ON	ON	ON	OFF	OFF	ON	72	OFF	ON	ON	OFF	ON	ON	ON
13	ON	ON	ON	ON	OFF	OFF	ON	73	OFF	ON	ON	OFF	ON	ON	OFF
14	ON	ON	ON	ON	OFF	OFF	OFF	74	OFF	ON	ON	OFF	ON	OFF	ON
15	ON	ON	ON	ON	OFF	OFF	OFF	75	OFF	ON	ON	OFF	ON	OFF	OFF
16	ON	ON	ON	OFF	ON	ON	ON	76	OFF	ON	ON	OFF	OFF	ON	ON
17	ON	ON	ON	OFF	ON	ON	ON	77	OFF	ON	ON	OFF	OFF	ON	OFF
18	ON	ON	ON	OFF	ON	ON	OFF	78	OFF	ON	ON	OFF	OFF	OFF	ON
19	ON	ON	ON	OFF	ON	ON	OFF	79	OFF	ON	ON	OFF	OFF	OFF	OFF
20	ON	ON	ON	OFF	ON	ON	ON	80	OFF	ON	OFF	ON	ON	ON	ON
21	ON	ON	ON	OFF	ON	ON	ON	81	OFF	ON	OFF	ON	ON	ON	OFF
22	ON	ON	ON	OFF	ON	ON	ON	82	OFF	ON	OFF	ON	ON	OFF	ON
23	ON	ON	ON	OFF	ON	ON	OFF	83	OFF	ON	OFF	ON	ON	OFF	OFF
24	ON	ON	ON	OFF	OFF	ON	ON	84	OFF	ON	OFF	ON	OFF	ON	ON
25	ON	ON	ON	OFF	OFF	ON	ON	85	OFF	ON	OFF	ON	OFF	ON	OFF
26	ON	ON	ON	OFF	OFF	ON	OFF	86	OFF	ON	OFF	ON	OFF	OFF	ON
27	ON	ON	ON	OFF	OFF	ON	OFF	87	OFF	ON	OFF	ON	OFF	OFF	OFF
28	ON	ON	ON	OFF	OFF	OFF	ON	88	OFF	ON	OFF	OFF	ON	ON	ON
29	ON	ON	ON	OFF	OFF	OFF	ON	89	OFF	ON	OFF	OFF	ON	ON	OFF
30	ON	ON	ON	OFF	OFF	OFF	OFF	90	OFF	ON	OFF	OFF	ON	OFF	ON
31	ON	ON	ON	OFF	OFF	OFF	OFF	91	OFF	ON	OFF	OFF	ON	OFF	OFF
32	ON	ON	ON	ON	ON	ON	ON	92	OFF	ON	OFF	OFF	OFF	ON	ON
33	ON	ON	ON	ON	ON	ON	ON	93	OFF	ON	OFF	OFF	OFF	ON	OFF
34	ON	ON	ON	ON	ON	ON	OFF	94	OFF	ON	OFF	OFF	OFF	OFF	ON
35	ON	ON	ON	ON	ON	ON	OFF	95	OFF	ON	OFF	OFF	OFF	OFF	OFF
36	ON	ON	ON	ON	ON	ON	ON	96	OFF	ON	ON	ON	ON	ON	ON
37	ON	ON	ON	ON	ON	ON	OFF	97	OFF	ON	ON	ON	ON	ON	OFF
38	ON	ON	ON	ON	ON	ON	OFF	98	OFF	ON	ON	ON	ON	OFF	ON
39	ON	ON	ON	ON	ON	ON	OFF	99	OFF	ON	ON	ON	ON	OFF	OFF
40	ON	ON	ON	ON	ON	ON	ON	100	OFF	ON	ON	ON	ON	ON	ON
41	ON	ON	ON	ON	ON	ON	OFF	101	OFF	ON	ON	ON	ON	ON	OFF
42	ON	ON	ON	ON	ON	ON	ON	102	OFF	ON	ON	ON	ON	OFF	ON
43	ON	ON	ON	ON	ON	ON	OFF	103	OFF	ON	ON	ON	ON	OFF	OFF
44	ON	ON	ON	ON	ON	ON	ON	104	OFF	ON	ON	ON	ON	ON	ON
45	ON	ON	ON	ON	ON	ON	OFF	105	OFF	ON	ON	ON	ON	ON	OFF
46	ON	ON	ON	ON	ON	ON	ON	106	OFF	ON	ON	ON	ON	ON	ON
47	ON	ON	ON	ON	ON	ON	OFF	107	OFF	ON	ON	ON	ON	ON	OFF
48	ON	ON	ON	ON	ON	ON	ON	108	OFF	ON	ON	ON	ON	ON	ON
49	ON	ON	ON	ON	ON	ON	ON	109	OFF	ON	ON	ON	ON	ON	OFF
50	ON	ON	ON	ON	ON	ON	OFF	110	OFF	ON	ON	ON	ON	ON	ON
51	ON	ON	ON	ON	ON	ON	OFF	111	OFF	ON	ON	ON	ON	ON	OFF
52	ON	ON	ON	ON	ON	ON	ON	112	OFF	ON	ON	ON	ON	ON	ON
53	ON	ON	ON	ON	ON	ON	OFF	113	OFF	ON	ON	ON	ON	ON	OFF
54	ON	ON	ON	ON	ON	ON	ON	114	OFF	ON	ON	ON	ON	ON	ON
55	ON	ON	ON	ON	ON	ON	OFF	115	OFF	ON	ON	ON	ON	ON	OFF
56	ON	ON	ON	ON	ON	ON	ON	116	OFF	ON	ON	ON	ON	ON	ON
57	ON	ON	ON	ON	ON	ON	OFF	117	OFF	ON	ON	ON	ON	ON	OFF
58	ON	ON	ON	ON	ON	ON	ON	118	OFF	ON	ON	ON	ON	ON	ON
59	ON	ON	ON	ON	ON	ON	OFF	119	OFF	ON	ON	ON	ON	ON	OFF
60	ON	ON	ON	ON	ON	ON	ON								

Mounting the SafeLINC FPII Card

Overview

The SafeLINC FPII card can be mounted to the 4100ES, 4100U, 4100, 4010ES, 4120, or 4020 systems. The mounting in each case is different. Refer to the appropriate topic in this section, depending on which fire alarm system you are using.

4100U/4100ES Mounting

The SafeLINC FPII assembly is to be mounted on the PDI in a 4100U/4100ES expansion bay (Figure 4). The card should be mounted to the left-most position on the PDI connector as Figure 4 illustrates.

Use the connector on the backside of the SafeLINC FPII card to connect to the bay as shown in Figure 4, below.

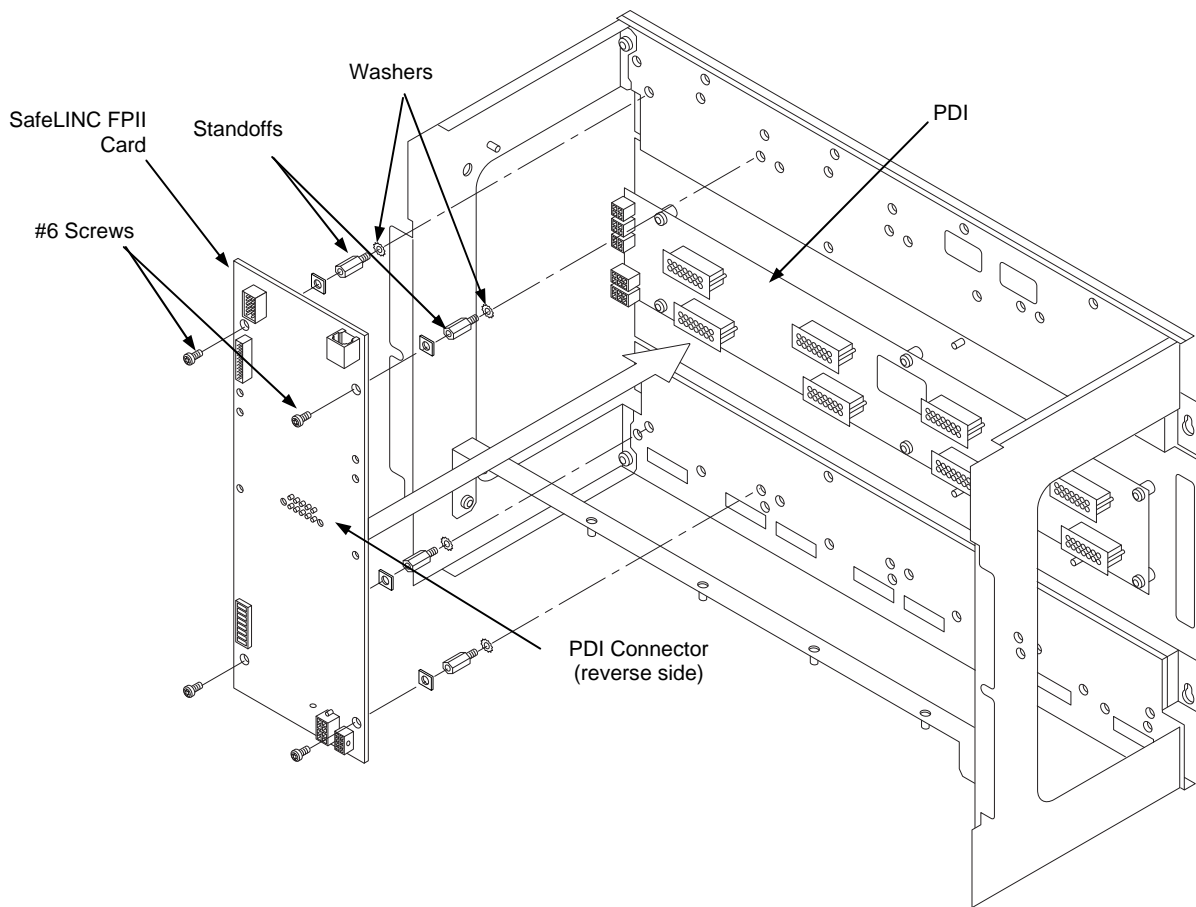


Figure 4. 4100U/4100ES Mounting

Mounting the SafeLINC FPII Card, *Continued*

4010ES Mounting

In the case of a 4010ES panel, it can be used inside a one-bay or two-bay panel. The FPII would be mounted on the top-bay or bottom-bay PDI card (Figure 5).

The SafeLINC FPII may mount in the left-most vertical block pair in a single-bay box or any open vertical block pair in a two-bay box.

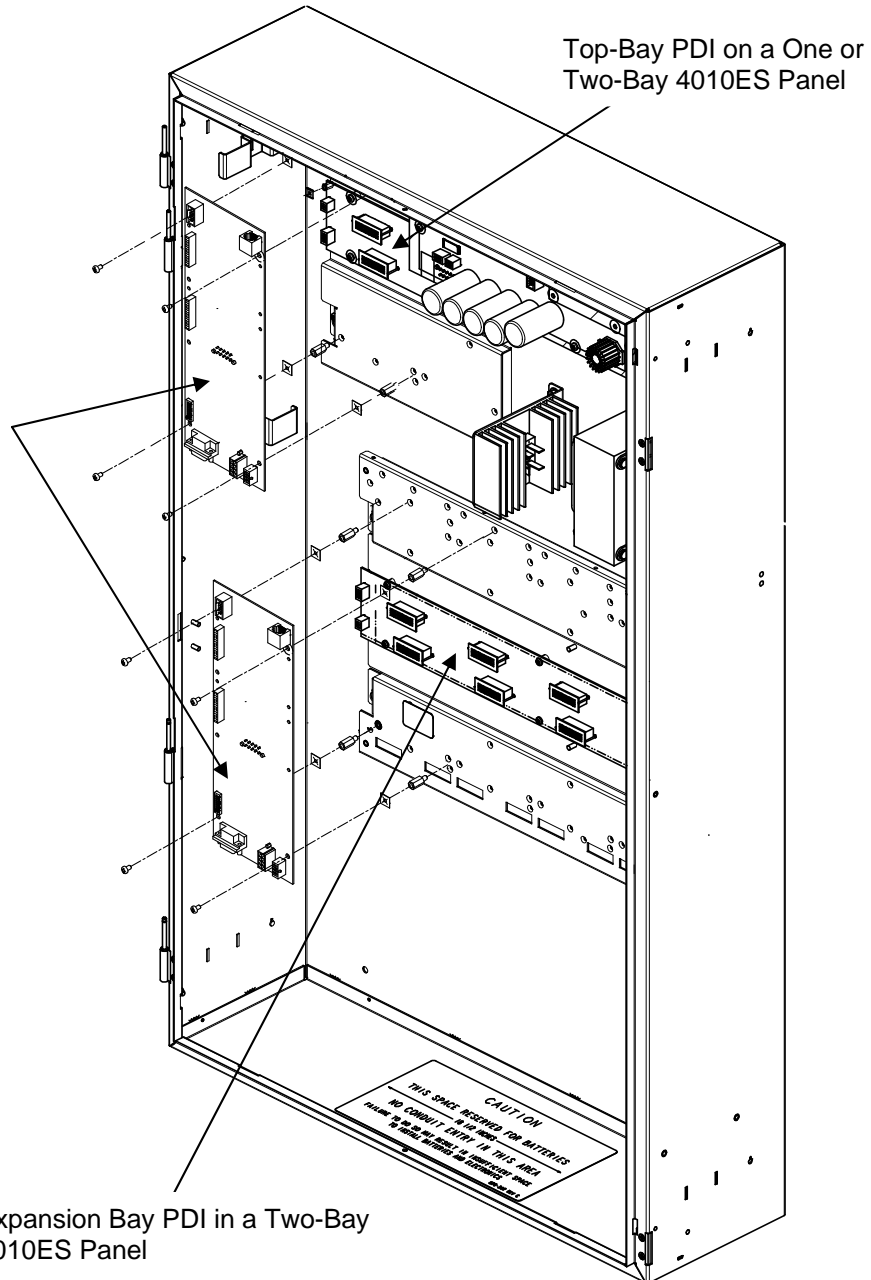


Figure 5. 4010ES Wiring

Mounting the SafeLINC FPII Card, *Continued*

4100/4120 Mounting

In either a 4100 or a 4120 system, the SafeLINC FPII takes up two 2-inch slots. Secure the assembly to the mounting rails as shown below.

Mount the card to the left-most position on the mounting rails (if possible).

IMPORTANT: The 637-591 Bracket must be mounted to the 4100/4120 mounting rails before the SafeLINC FPII card is mounted.

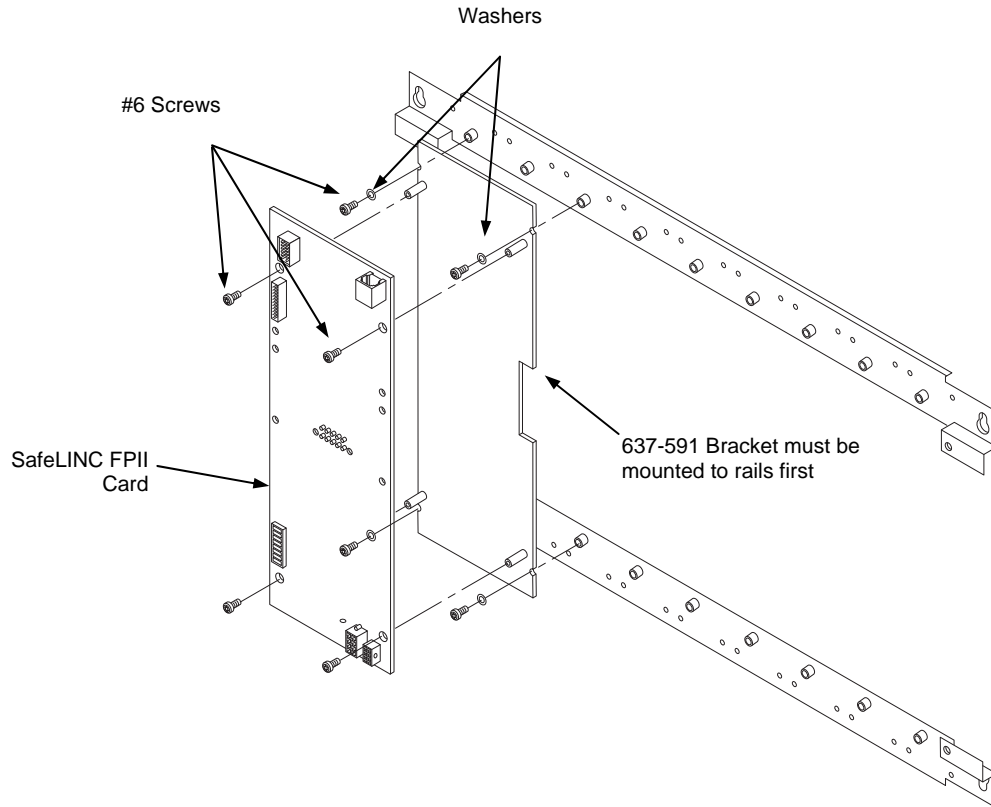


Figure 5. 4100/4120 Mounting

Mounting the SafeLINC FPII Card, *Continued*

4020 Mounting

In a 4020 system, the SafeLINC FPII assembly mounts onto either the back plate or hat bracket as shown below.

Mount the card to the left-most position on the mounting rails (if possible).

IMPORTANT: If a hat bracket is installed, the SafeLINC FPII assembly **must** be mounted to the hat bracket.

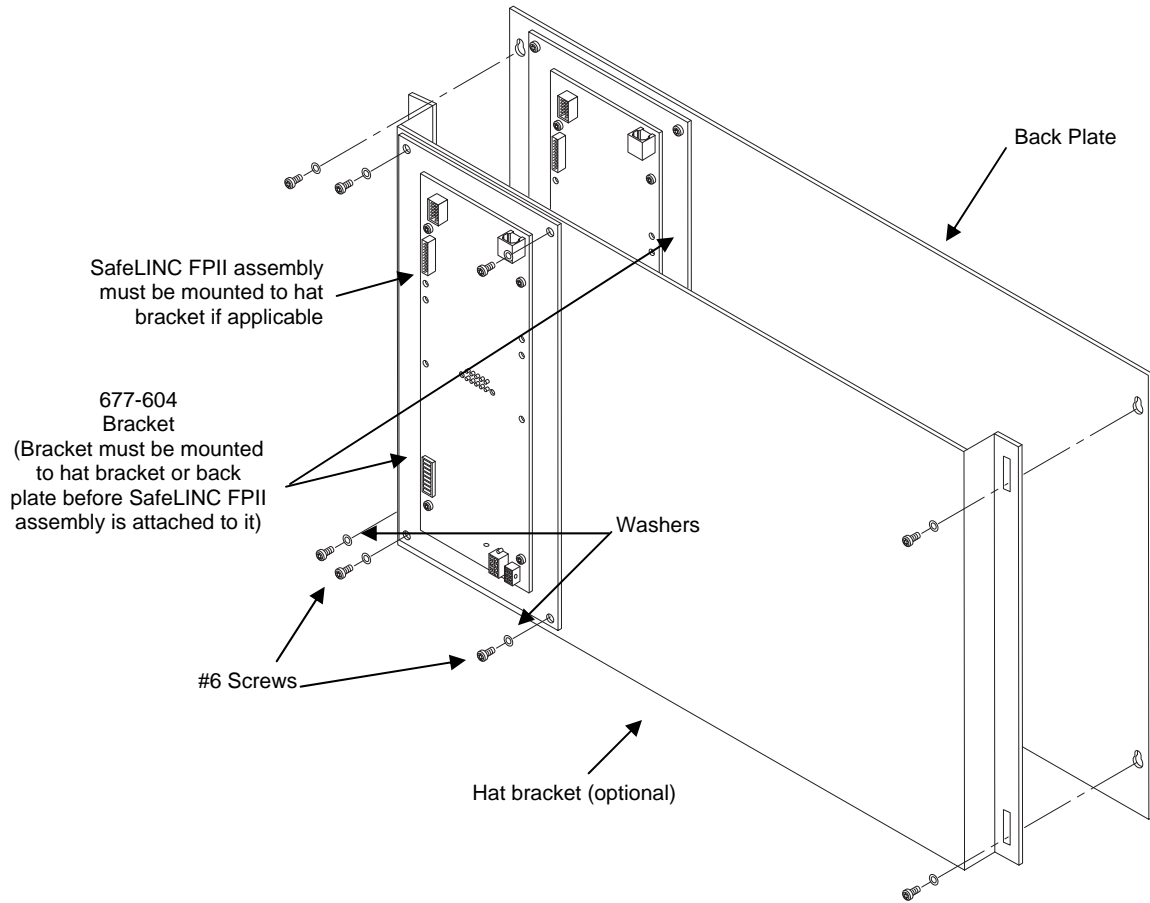


Figure 6. 4020 Mounting

SafeLINC FPII Field Wiring

Overview

This section contains the complete field wiring drawings for the SafeLINC FPII card.

4100U/4100ES/ 4010ES-Style Wiring

The SafeLINC FPII card can connect to 4100U/4100ES and 4010ES PDI boards as shown below. Unlike the 4100/4120 and 4020, a harness is not required for power and communications.

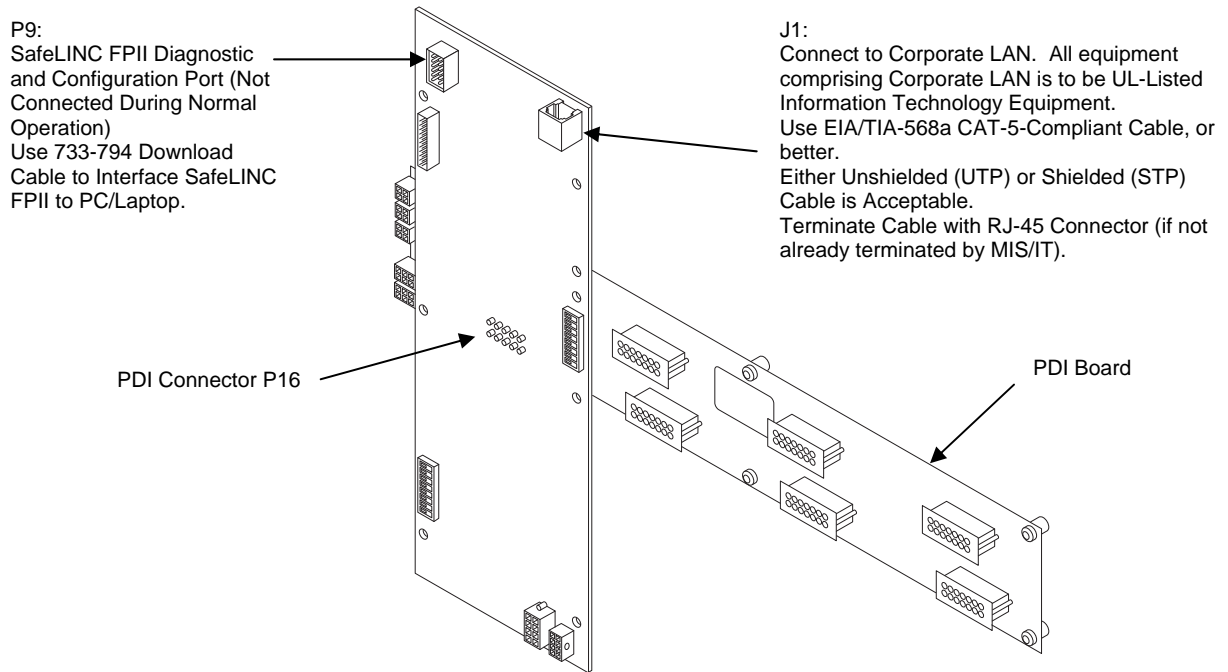


Figure 7. 4100U/4100ES and 4010ES-Style Wiring

SafeLINC FPII Field Wiring, *Continued*

4100/4120 Legacy Wiring

The SafeLINC FPII card can connect to 4100/4120 Legacy (non-4100U/4100ES) motherboards as shown below.

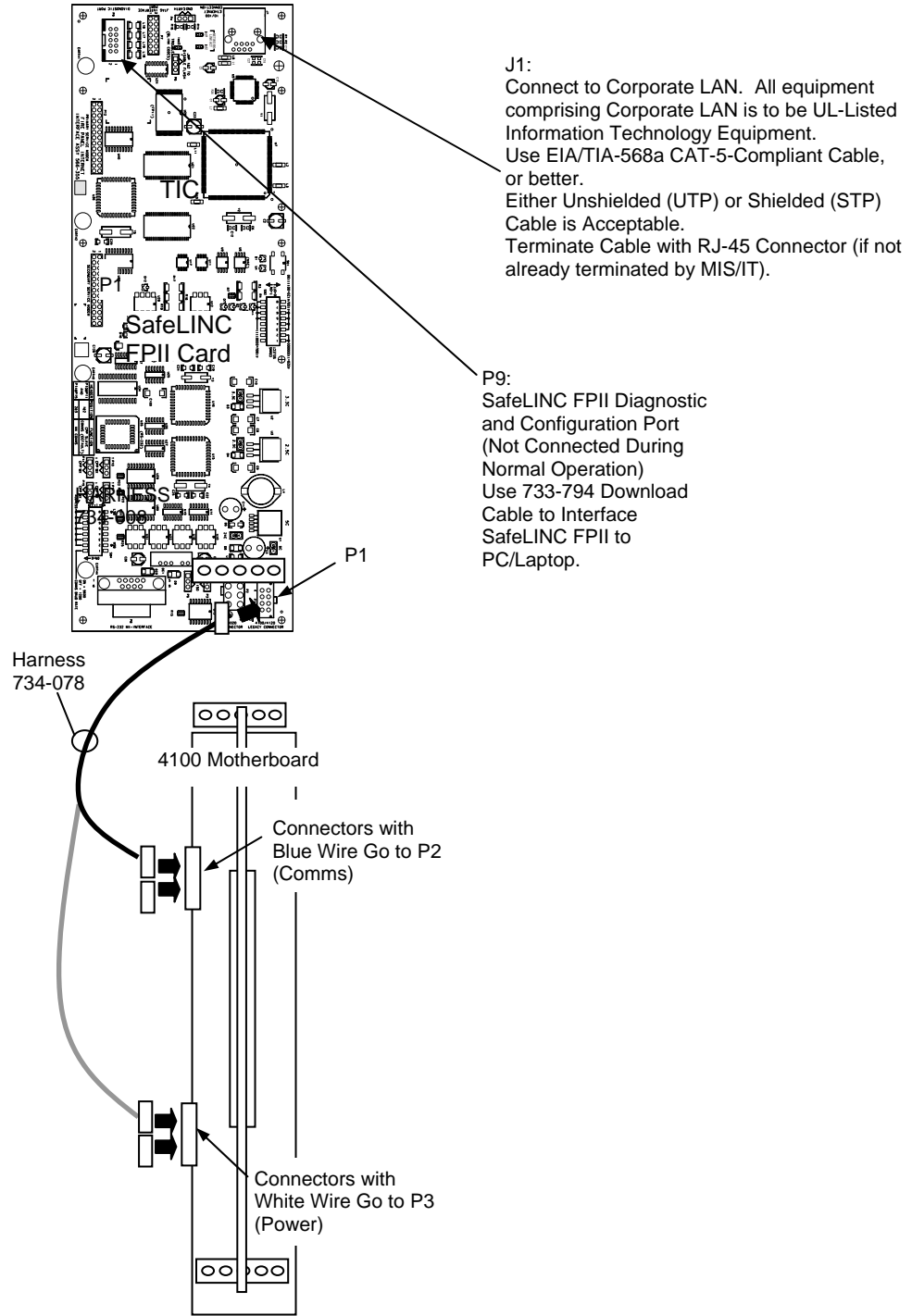


Figure 8. 4100/4120 Legacy Wiring

SafeLINC FPII Field Wiring, *Continued*

4020-Style Wiring

The SafeLINC FPII card can connect to a 4020 as shown in Figure 9. This illustration shows the SafeLINC FPII card connected to MAPNET Interface Board via Harness 733-693 and the 4020 Power & Comms Connector P2. This is an example of one connection to the 4020. If the MAPNET Interface Board is unavailable for power and communications, you will need to connect to another 4020 board. Instead of the MAPNET Interface Board, you also can connect Harness 733-693 from the SafeLINC FPII's P2 connector to the Standard Slave Card (P6, P7), Power Supply Interface Board (P2, P3), 8-Point I/O Board (P9, P10), 2120/RS232 Interface Board (P8, P9), or Network Option Board/Repeater Card (P11, P12). See the 4020 Interconnection Diagrams (841-906) for more information.

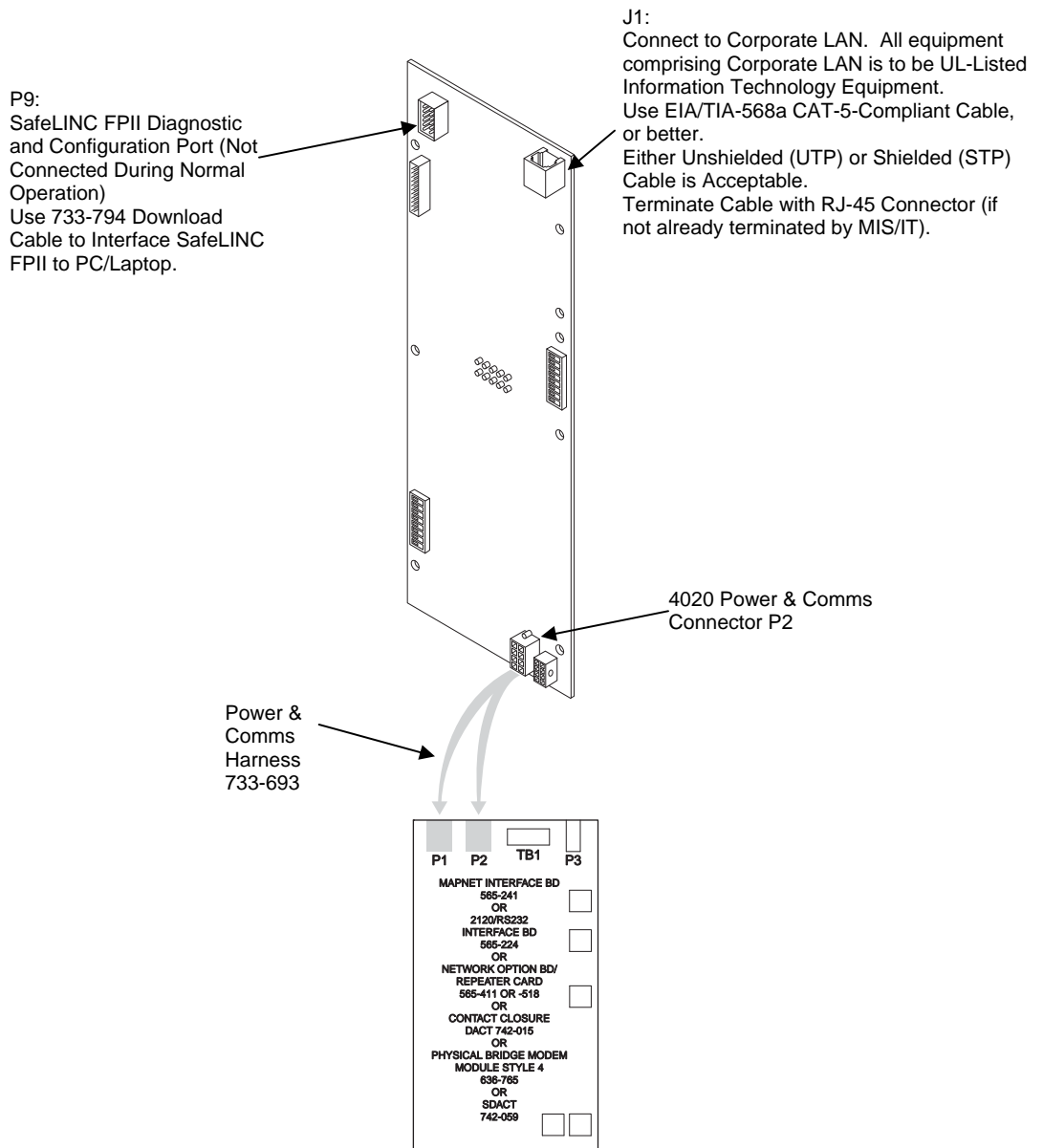


Figure 9. 4020-Style Wiring

LED Indicators

Interpreting LED Indications

The SafeLINC FPII contains 3 LEDs to provide user status indication. (See Figure 1 for location of LEDs.) LED 3, colored yellow, provides trouble status information using blink codes. The summary of the blink codes (trouble codes) appears in Table 3 below.

LEDs 1 and 2 are used to monitor both the integrity of the network connection (Link Status, Green LED = LED1) and whether network activity is present (Network Activity, Red LED = LED2) to and from the SafeLINC FPII.

Table 3. Blink Codes for LED 3 (Yellow LED)

LED	Blink Code	Definition (See below for more details)
LED3 (Yellow LED)	Short-Short-Short	Network Down (Network Status Check Trouble)
	Short-Long-Short	Network Disconnected (Network Link Integrity Trouble)
	Short-Long-Long	Internal Network Loop-Back Trouble
	Short-Short-Long	Email Link Trouble
	Long-Long-Long	RUI/4100 Comms or Slave Core Trouble
	Long-Short-Short	RAM Test Trouble
	Long-Short-Long	FLASH Test Trouble
	Long-Long-Short	EEPROM Test Trouble
Notes: Short = ½-second duration Long = 1-second duration Rest between multiple troubles = 2 seconds Rest between repeating trouble list = 3 seconds.		

Network Down (Network Status Check) - Used as a diagnostic to determine if the SafeLINC FPII can see out onto the connected network, the SafeLINC FPII periodically checks the customer’s configured gateway (as was configured on the boot prompt) to verify that the SafeLINC FPII can see the gateway. However, it does not guarantee that the SafeLINC FPII is fully operational on the network to which it is connected. The frequency of this check is determined by configuring the Network Status Check under Administration: Security Settings.

Network Disconnected (Network Link Integrity) - The SafeLINC FPII examines the Link Integrity Bit on the PHY to determine if the Ethernet Cable is plugged into the SafeLINC FPII. If the cable is plugged into both the Hub/Router/Switch and the SafeLINC FPII, the Green Link LED (LED1) will light up. There is no configurable option on the web pages for this diagnostic feature. The SafeLINC FPII checks this at the same interval as configured for Network Down (Network Status Check Trouble).

Internal Local Loop-Back - Testing the integrity of the onboard connection from the microprocessor to the Ethernet Connector, the SafeLINC FPII takes an outgoing test packet and re-routes it internally to the PHY and then back to the microprocessor. This test determines if the PHY & MAC are operational. Between this test and the Network Disconnected Test (Network Link Integrity Test), you are reasonably sure that the SafeLINC FPII can communicate on the network as long as it has been configured properly.

Email Link – Periodically testing for the presence of the email server to see if it is able to accept messages, this diagnostic logs into the SMTP server and logs out without sending any email messages. This testing interval is defined under SafeLINC FPII: SafeLINC FPII Administration: Email Configuration as the Email Health Status Check Interval. This test also checks that the PC on which the server is running is operational as well as checking that the SMTP server is actually running, too. Although this test does not check that the remaining network is operational, it does reasonably ensure that any email message can be delivered to the server successfully.

Continued on next page

LED Indicators, *Continued*

Interpreting LED Indications

RUI/4100 Comms or Slave Core – This is the same trouble information that the RS232 card normally reports. The signal line is brought into the SafeLINC FPII so that it can be monitored for trouble reporting on the RS232 card. This line is monitored continuously during boot-up and run-time because the RS232 is communicating to the host FACP during these times. When this trouble is active, a trouble will be reported to the host FACP.

RAM Test – Conducted only at boot-up and characterized by the long continuous illumination of LED3 while the test is ensuing, this test covers the entire contents of the DRAM (both U21 and U22) on the SafeLINC FPII to ensure that the memory integrity is intact.

FLASH Test – Conducted only at boot-up and characterized by the long continuous illumination of LED3 while the test is ensuing, this test covers the entire contents of the FLASH (U20) on the SafeLINC FPII to ensure that the memory integrity is intact.

EEPROM Test - Conducted only at boot-up and characterized by the long continuous illumination of LED3 while the test is ensuing, this test covers the entire contents of the Serial EEPROM (U6) on the SafeLINC FPII to ensure that the memory integrity is intact.

Adding the SafeLINC FPII to the FACP via the Programmer

Overview

The following sections describe how to add the SafeLINC FPII to the FACP via the DOS-based Programmer or the Windows-based Programmer. You will select a method (DOS or Windows) according to what FACP will have the SafeLINC FPII installed in it. For example, the 4100U/4100ES and 4010ES FACPs with installed SafeLINC FPII will require the Windows-based Programmer.

These sections are not intended to teach you how to use each Programmer; rather, they will point out the important information that's necessary to build a job properly to support the SafeLINC FPII.

Using the DOS-Based Programmer

This section shows you how to add the SafeLINC FPII to a compatible FACP using the DOS-based Programmer.

The SafeLINC FPII is configured in the 4100 Programmer as an Interface card type (similar to an RS232, MAPNET, etc.). Data entry for the card is also similar to the RS232 with certain limitations.

Use Steps 1 through 16 below to add a SafeLINC FPII to the FACP.

1. Use a PC with the DOS-based 4100 Programmer application installed or install the application on your PC. If necessary, refer to Publication 574-102 (4100 Programming Instructions, Version 8.01) or Publication 579-127 (4100 Fire Alarm Programming Unit Supplement, Version 9) for installation instructions on the 4100 Programmer application.
2. Start up the 4100 Programmer on your PC by selecting the Start button from Windows, and then selecting Programs, Simplex, and 4100 Programmer.
3. Load a specific job from the **Utilities** menu.
4. After the job is successfully loaded, use the arrow keys to select the **Configuration** menu and press Enter (see Figure 10). If creating a new job, see the aforementioned Publications 574-102 or 579-127 for more information if needed.

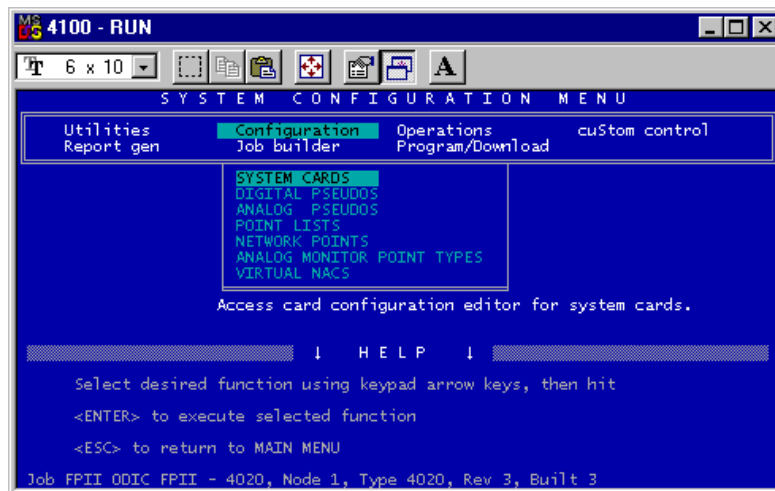


Figure 10. System Configuration Menu

Continued on next page

Adding the SafeLINC FPII to the FACP via the Programmer, *Continued*

Using the DOS-Based Programmer

- Using the arrow keys, select the **System Cards** menu and press Enter (see Figure 10).
- Press A to add the SafeLINC FPII card. Figure 11 shows the card added as a 2120/RS232 Interface Card. With this card highlighted, press Enter to go to the 2120 Interface/RS232 Card Data Entry Screen

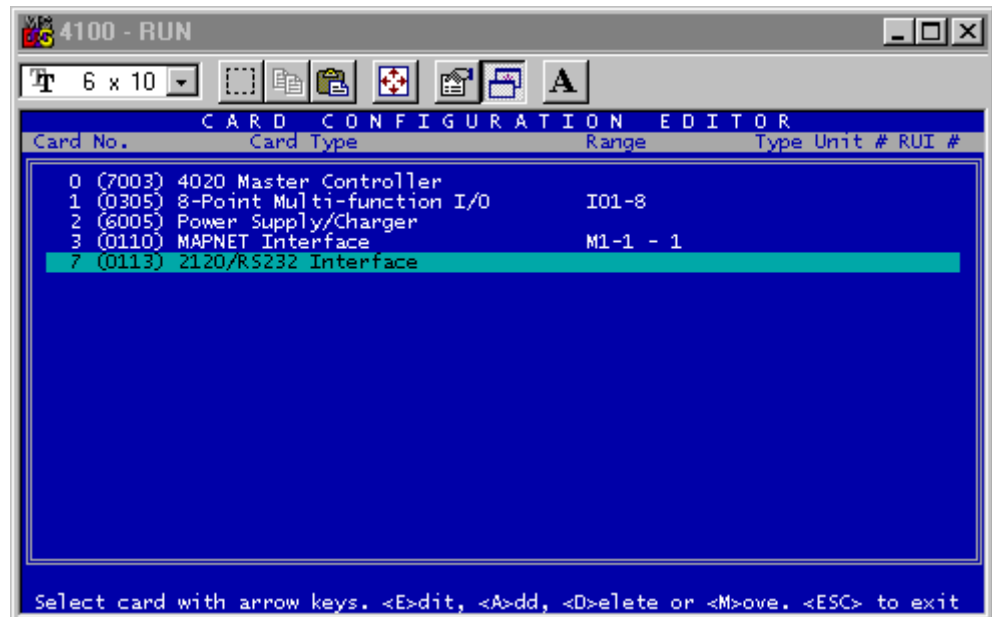


Figure 11. Card Configuration Editor

- Press E to edit the communication settings (see Figure 12).

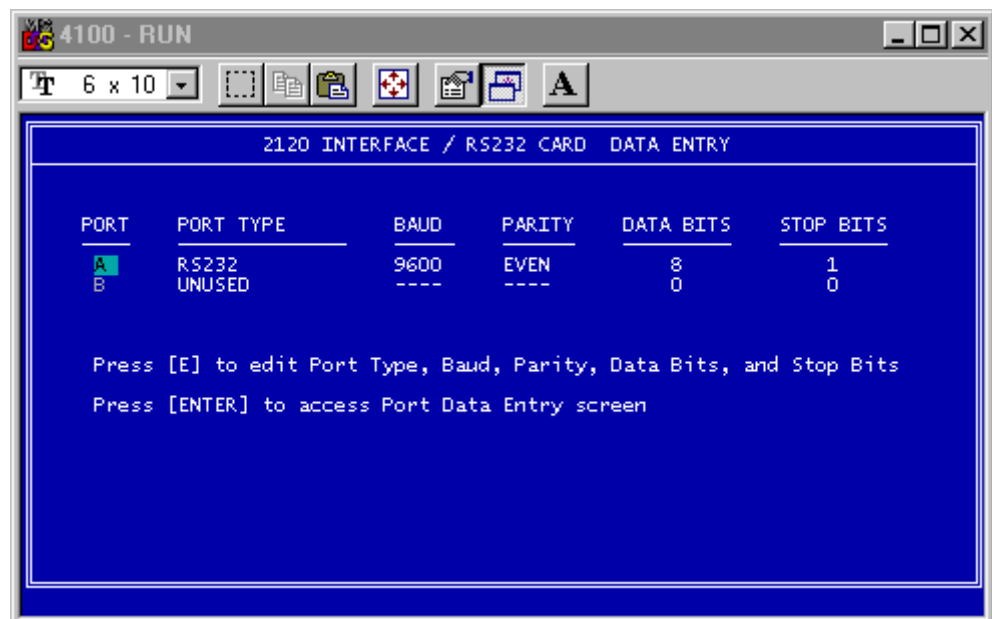


Figure 12. Communication Settings

Continued on next page

Adding the SafeLINC FPII to the FACP via the Programmer, *Continued*

Using the DOS-Based Programmer

- Configure Port A as shown in Figure 12 (9600 Baud, Even Parity, 8 Data Bits, and 1 Stop Bit). (Since Port B is not supported, you need to leave it unused.)
- Press Enter to access the RS232 Port Data Entry screen (see Figure 13).

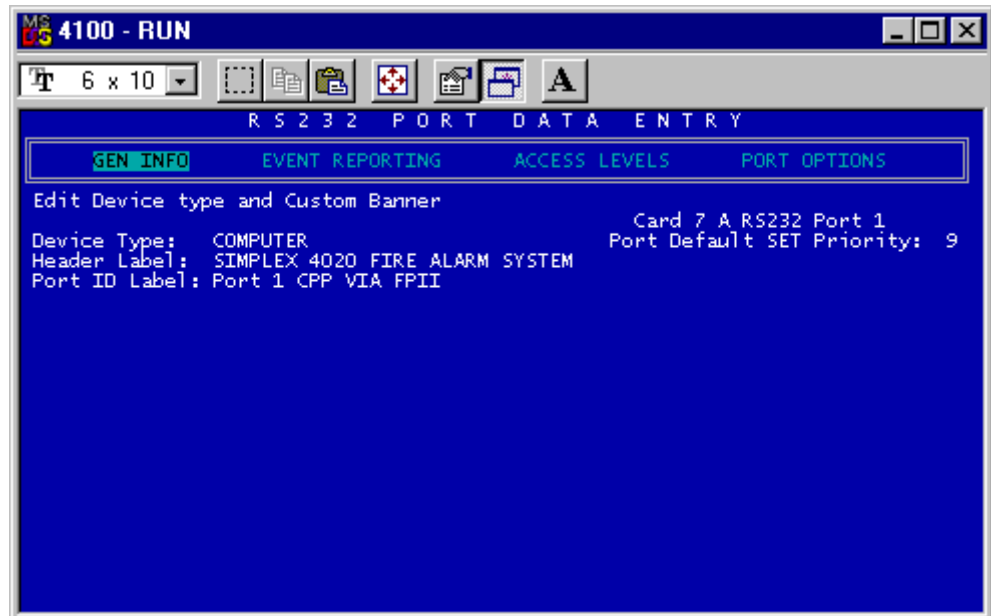


Figure 13. RS232 Port Data Entry Screen

- Choose **Computer** for device type, and type in a header label and port ID label. When done, use the arrow keys to select the **Event Reporting** option (see Figure 14).

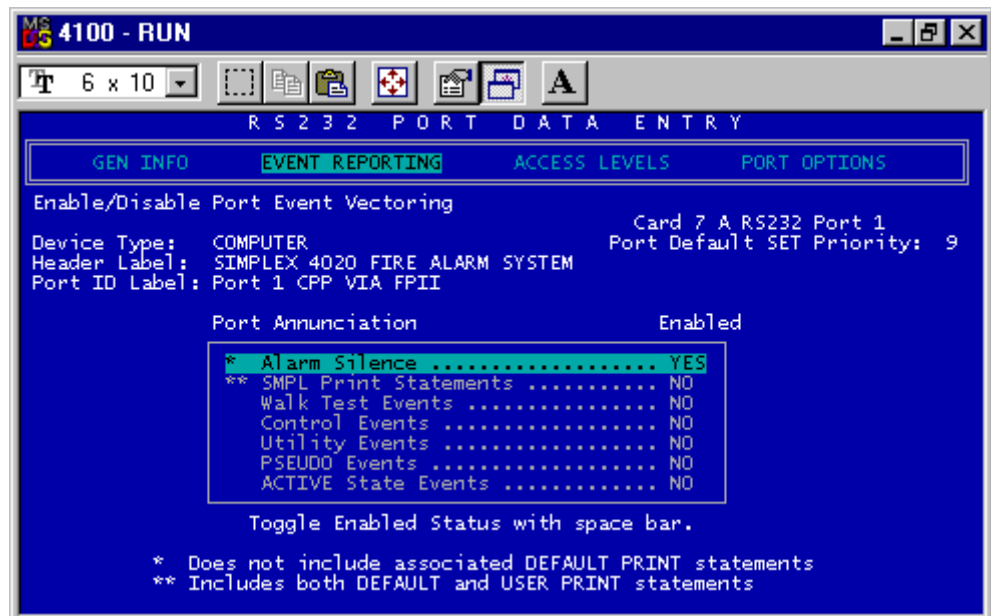


Figure 14. Event Reporting Option

Continued on next page

Adding the SafeLINC FPII to the FACP via the Programmer, *Continued*

Using the DOS-Based Programmer

- Using the space bar to toggle between selections, enable Fire Alarm, Trouble, Supervisory, and Priority 2 Alarm Events as well as System Reset and Alarm Silence by choosing YES. Leave the remaining event types disabled. See Figure 14.
- After saving the option settings by using the Escape key and answering prompts, use the arrow keys to select **Access Levels** option (see Figure 15).

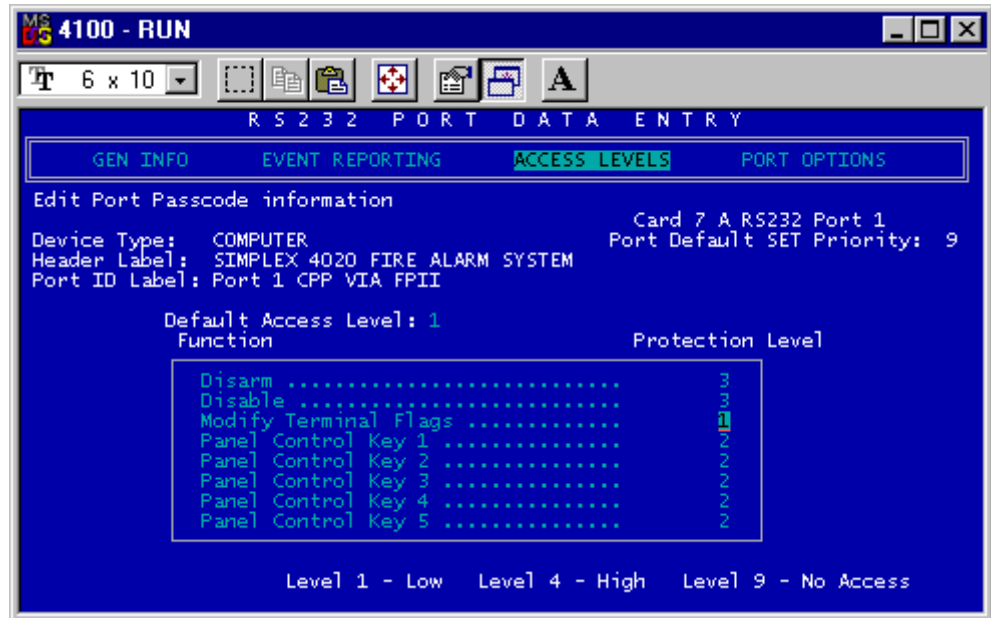


Figure 15. Access Levels Option

- Make needed modifications to the access levels except for Modify Terminal Flags. You must set Modify Terminals Flags to 1.

NOTE: No user will have direct access to the Computer Port Protocol (CPP) via the SafeLINC FPII.

- After saving the function settings by using the Escape key and answering prompts, use the arrow keys to select **Port Options** option (see Figure 16).

Continued on next page

Adding the SafeLINC FPII to the FACP via the Programmer, *Continued*

Using the
DOS-Based
Programmer

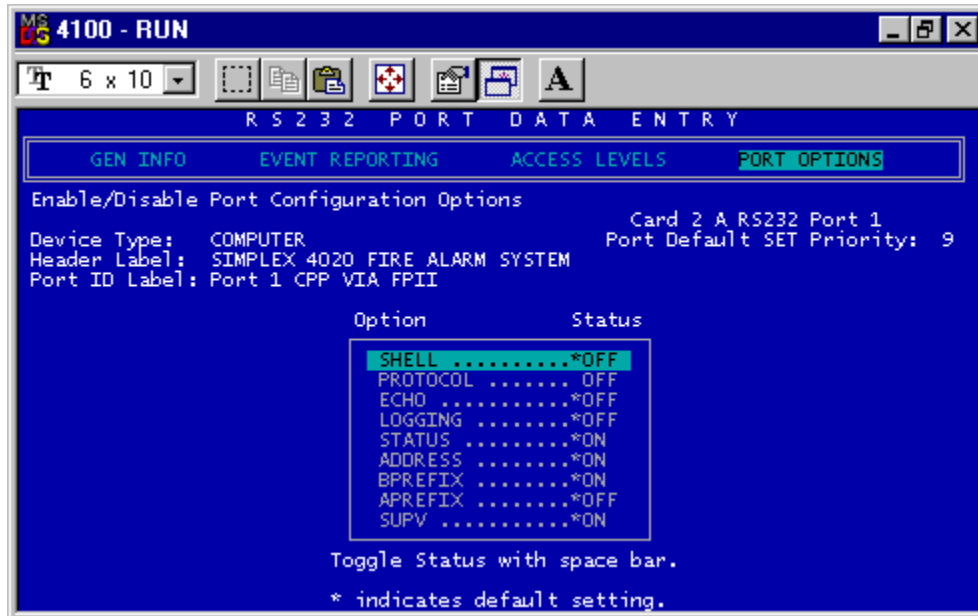


Figure 16. DOS Port Options

15. Modify the terminal flags as shown in Table 4.

Table 4. Terminal Flag Settings

Terminal Flag Description	Setting
SHELL	OFF
PROTOCOL	OFF
ECHO	OFF
LOGGING	OFF
STATUS	ON
ADDRESS	ON
BPREFIX	ON
APREFIX	OFF
SUPV	ON
BELLS	OFF
HSHAKE	OFF
POLL	OFF
ATTRIB	ON
LINE FEED	ON
LINE WIDTH	80

16. Return to the **Utilities** menu. Use the arrow keys to select **Save Current Job** from the **Utilities** menu and press Enter, or continue to build the job as necessary. The SafeLINC FPII configuration portion is now complete.

Adding the SafeLINC FPII to the FACP via the Programmer, *Continued*

Using the Windows-Based Programmer

This section shows you how to add the SafeLINC FPII to a compatible FACP using the Windows-based Programmer.

The SafeLINC FPII is configured in the Programmer as an Interface card type (similar to an RS232, MAPNET, etc.). Data entry for the card is also similar to the RS232 with certain limitations.

Use Steps 1 through 16 below to add a SafeLINC FPII to the FACP.

NOTE: The dialog boxes shown are for the 4100U jobs and they are identical for the 4010ES jobs, except the dialog box header which shows the proper PID.

1. Use a PC with the Windows-based Programmer application installed or install the application on your PC. If necessary, refer to the *ES Panel Programmer's Manual* (574-849) for installation instructions on the Programmer application.
2. Run the Panel Programmer on your PC.
3. Load a specific 4100U, 4100ES or 401ES job (...create new job).
4. Using the Hardware tab, add a 2120/RS232 Interface Card. The SafeLINC FPII is added like a 2120/RS232 Interface Card; however, the SafeLINC FPII only supports just a subset of the features supported by a 2120/RS232 Interface Card. Figure 17 shows a card already added near the bottom of the screen.

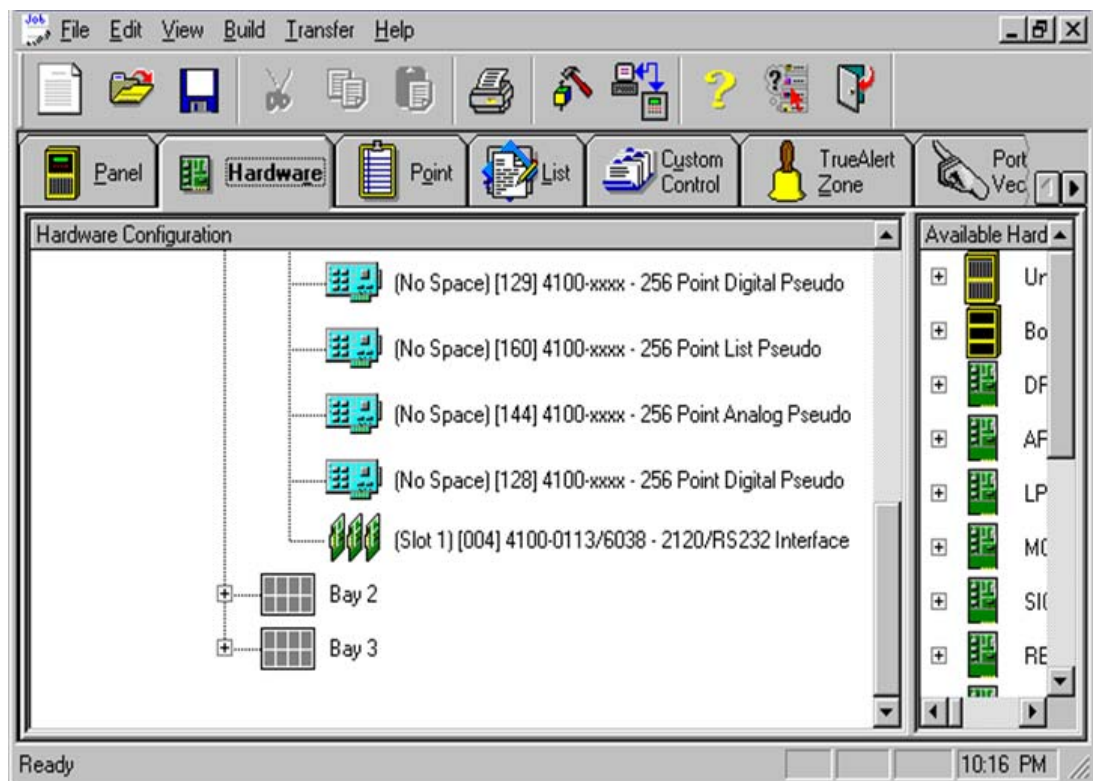


Figure 17. Hardware Configuration (4100U software shown)

Continued on next page

Adding the SafeLINC FPII to the FACP via the Programmer, *Continued*

Using the Windows-Based Programmer

5. Double click the 2120/RS232 Interface Card (see Figure 18).

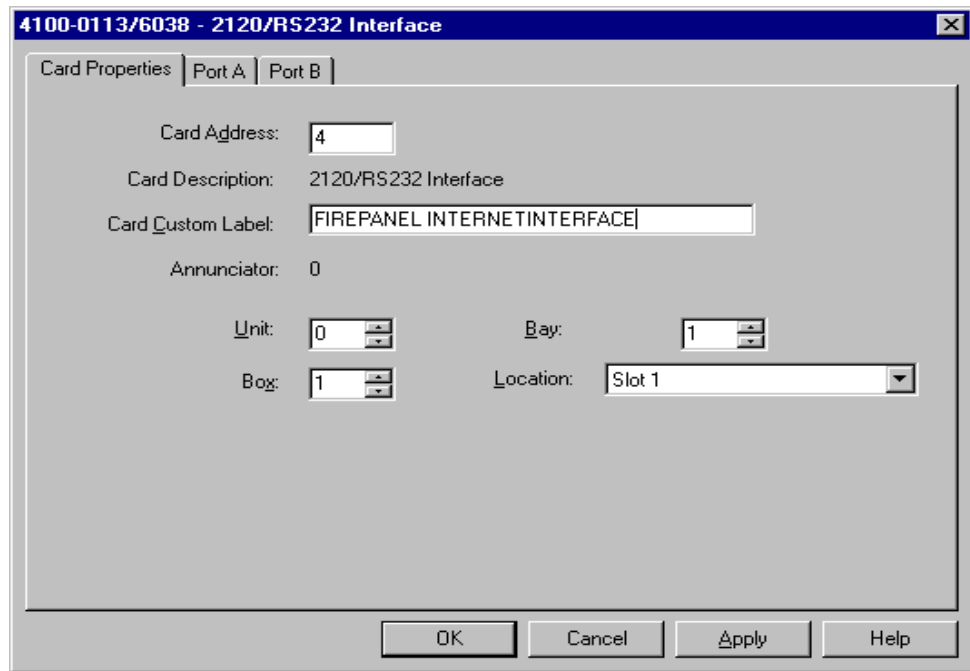


Figure 18. Custom Label Information

6. Type in Custom Label information as shown in Figure 18.
7. Click on the Port A tab, and then configure Port A as shown in Figure 19 (9600 Baud, Even Parity, 8 Data Bits, and 1 Stop Bit). (Since Port B is not supported, you need to leave it unused.)

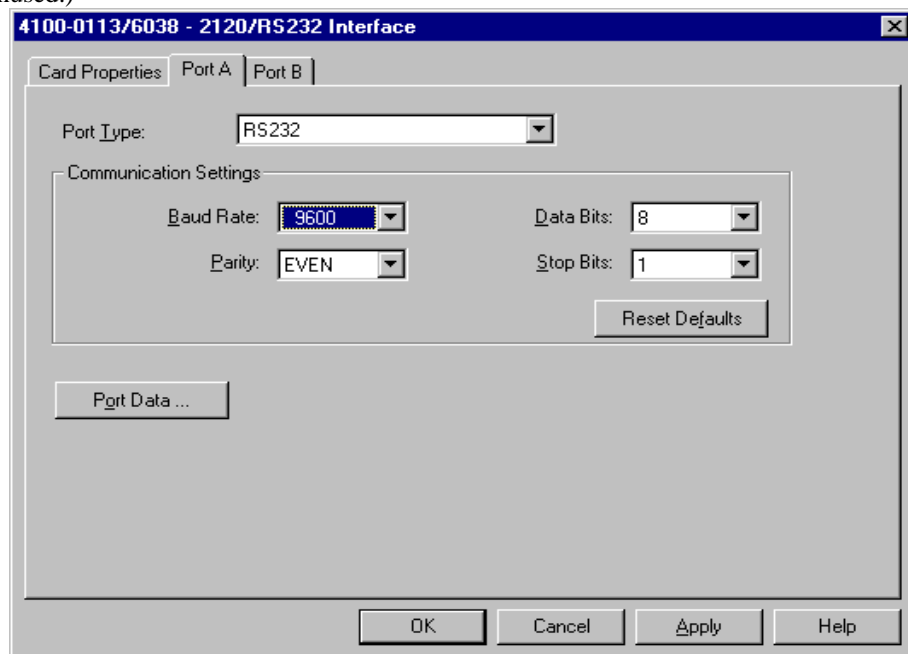


Figure 19. Communication Settings

Continued on next page

Adding the SafeLINC FPII to the FACP via the Programmer, *Continued*

Using the Windows-Based Programmer

- Click on the Port Data button to access the RS232 Port Data Entry screen (see Figure 20).

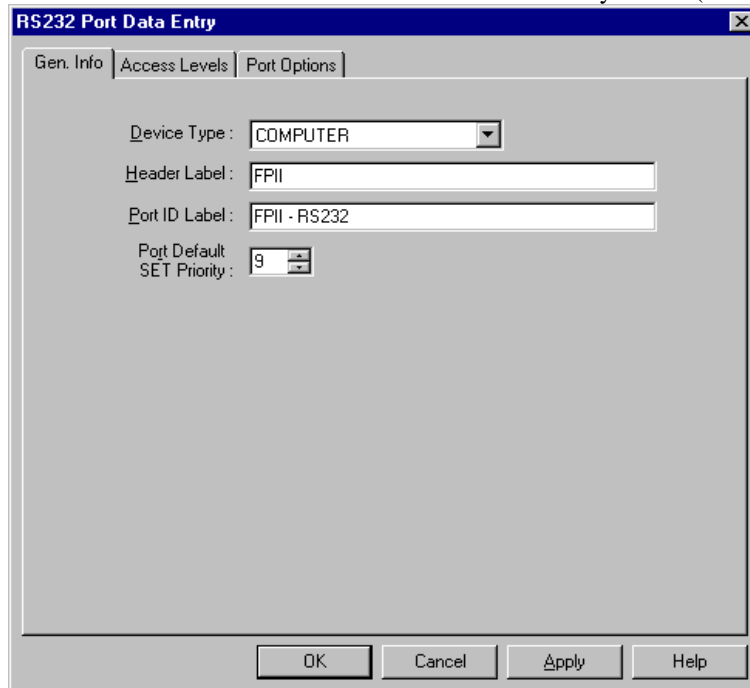


Figure 20. RS232 Port Data Entry Screen

- Choose **Computer** for device type, and type in a header label and port ID label. When done, click on the **Access Levels** tab (see Figure 21).

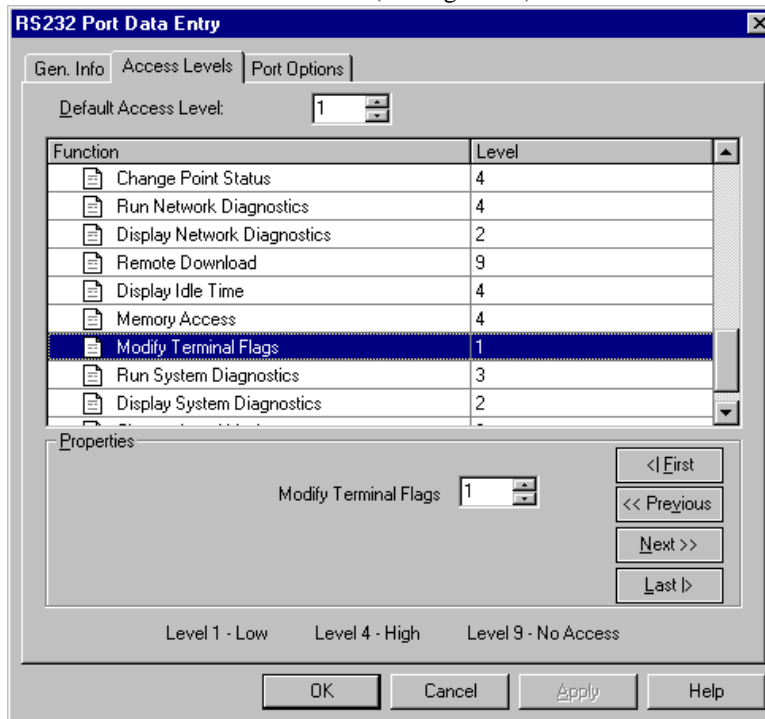


Figure 21. Access Levels Option

Continued on next page

Adding the SafeLINC FPII to the FACP via the Programmer, *Continued*

Using the Windows-Based Programmer

- Make needed modifications to the access levels except for Modify Terminal Flags. You must set Modify Terminals Flags to 1.

NOTE: No user will have direct access to the Computer Port Protocol (CPP) via the SafeLINC FPII.

- Click on the **Port Options** tab (see Figure 22).

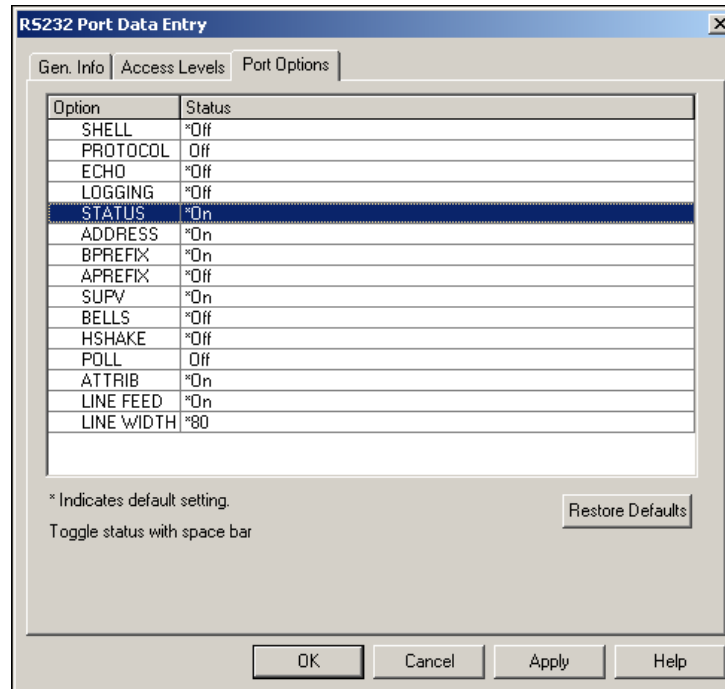


Figure 22. Port Options

- Modify the terminal flags as shown in Table 5.

Table 5. Terminal Flag Settings

Terminal Flag Description	Setting
SHELL	OFF
PROTOCOL	OFF
ECHO	OFF
LOGGING	OFF
STATUS	ON
ADDRESS	ON
BPREFIX	ON
APREFIX	OFF
SUPV	ON
BELLS	OFF
HSHAKE	OFF
POLL	OFF
ATTRIB	ON
LINE FEED	ON
LINE WIDTH	80

- Click the OK button and then click the OK button at the next screen to return to the main Programmer screen.

Continued on next page

Adding the SafeLINC FPII to the FACP via the Programmer, *Continued*

Using the Windows-Based Programmer

- Click the Port Vectoring tab and then highlight the RS232 card (not the Service Port selection).

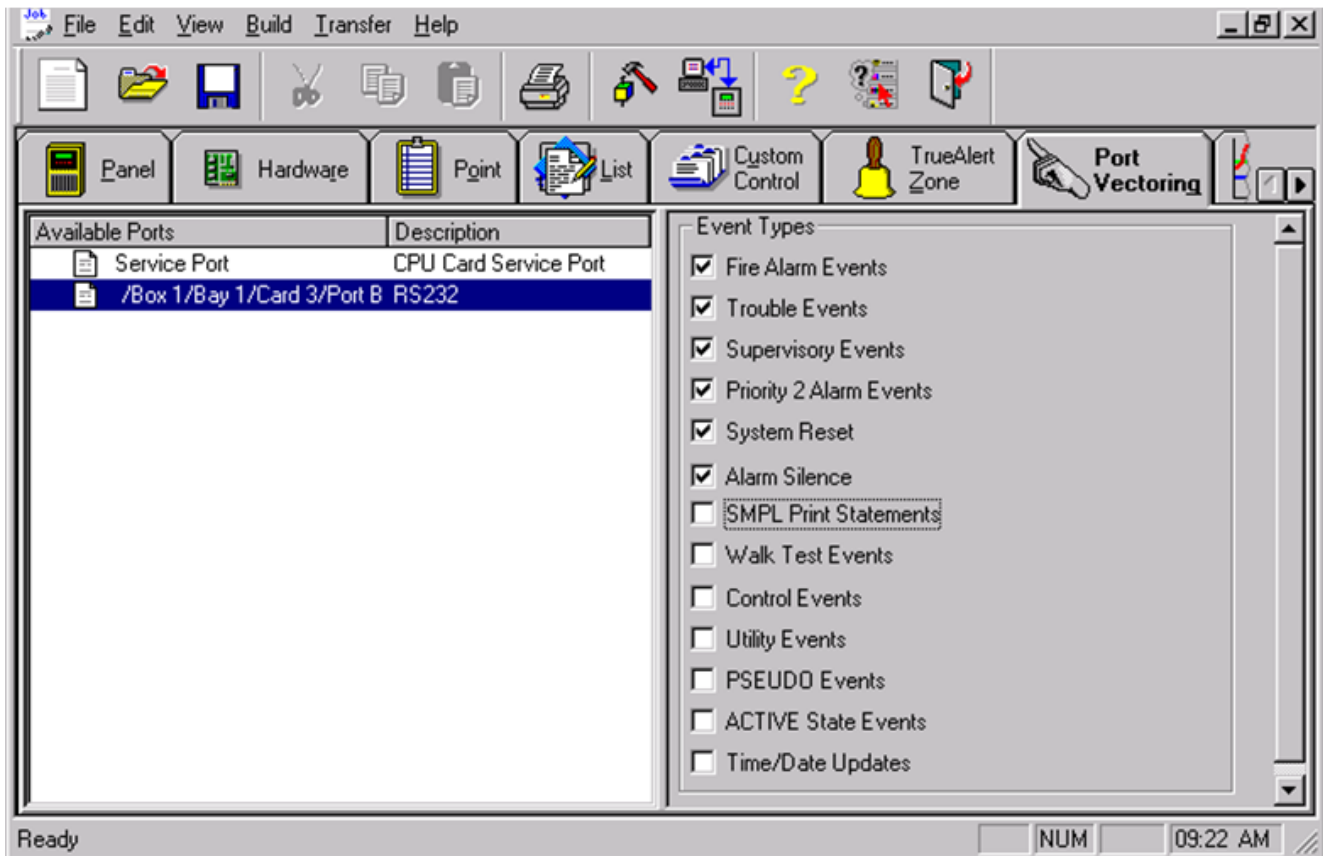


Figure 23. Event Reporting Option (4100U software shown)

- As shown in Figure 23, enable the Fire Alarm, Trouble, Supervisory, and Priority 2 Alarm Events as well as System Reset and Alarm Silence by checking off the field next to each event type. Leave the remaining event types disabled.
- Save the job or continue to build the job as necessary. The SafeLINC FPII configuration portion is now complete.

Connecting a PC to the SafeLINC FPII Diagnostic & Configuration Port

Connecting SafeLINC FPII Card to a PC

The SafeLINC FPII card must be connected to a PC to configure the basic settings. The PC must meet the requirements of UL-Listed Information Technology Equipment. Use Download Cable 733-794 to connect P9 on the SafeLINC FPII card to the PC.

- Align red stripe on Download Cable with Pin 1 on P9.

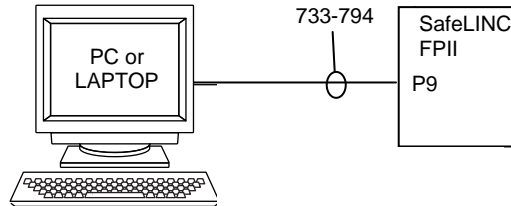


Figure 24. Connecting SafeLINC FPII Card to PC

Configuring a Terminal Emulation Program

Hyperterm is a terminal emulation program available under all Windows platforms.

Configure the Hyperterm or equivalent Terminal Emulation program to run at 19.2K, 8-N-1 with no hardware handshaking. Under settings, configure emulation to Auto Select.

Note: Some users may experience difficulties with Auto Select. If you are one of these users, please change to VT-100 emulation.

Checking for Duplicate IP Addresses

Before you configure the SafeLINC FPII on the boot prompt, you need to check out if the MIS/IT configured IP address for where you intend to install the SafeLINC FPII is active on the network.

Since the SafeLINC FPII is not yet operational at this point, you should not be able to successfully communicate with the assigned IP address. To perform this check, you will use a Windows Utility called Ping.

- Open a DOS Window on any PC connected to same LAN as the SafeLINC FPII.
- At the DOS Prompt, type in: **ping ip_address**

Substitute the *ip_address* parameter for the actual IP Address assigned by the MIS/IT Department for the SafeLINC FPII. For example, ping 192.168.0.1 and press Enter.

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 25. Expected Results (No Device Response to Ping Command)

Continued on next page

Connecting a PC to the SafeLINC FPII Diagnostic & Configuration Port, *Continued*

Checking for Duplicate IP Addresses

If you do not see a device responding to your Ping command as shown in Figure 25, the test is complete and you may proceed to configure the SafeLINC FPII to operate on the local network. The results in Figure 25 indicate that there is no other device on the network responding to the address provided by the MIS/IT Department. Proceed to configure the SafeLINC FPII.

```
C:\>ping 10.26.3.194

Pinging 10.26.3.194 with 32 bytes of data:

Reply from 10.26.3.194: bytes=32 time<10ms TTL=60
Reply from 10.26.3.194: bytes=32 time<10ms TTL=60
Reply from 10.26.3.194: bytes=32 time<10ms TTL=60
Reply from 10.26.3.194: bytes=32 time<10ms TTL=60

Ping statistics for 10.26.3.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 26. Unexpected Results (Device Response to Ping Command)

However, if you do see a device responding to your Ping command as shown in Figure 26, contact the MIS/IT Department. ***DO NOT attempt to configure the SafeLINC FPII on the network until the problem is fixed.***

Using the Boot Menu

Completing the MIS/IT Configuration Worksheet

Before using the SafeLINC FPII, the SafeLINC FPII must be configured for use via a terminal emulation program. Follow the instructions below.

1. Reboot the FACP and press any key to interrupt the SafeLINC FPII boot procedure. For Rev. B and later SafeLINC FPII cards, you may press SW1 on the SafeLINC FPII card before pressing any key to interrupt the SafeLINC FPII boot procedure.
 - The MAC address is displayed initially during SafeLINC FPII boot procedure. See Figure 27. (The SafeLINC FPII can take several minutes to display the contents shown in Figure 27. The delay is due to the hardware diagnostics performed during the boot procedure.)

```
SafeLINC Fire Panel Internet Interface (FPII)
Boot Procedure in Progress:
SafeLINC FPII System Firmware Revision 2.00.19

SafeLINC FPII Static IP Address...: 10.26.3.194
SafeLINC FPII Subnet Mask.....: 255.255.0.0
SafeLINC FPII Default Gateway....: 10.26.1.254

MAC Address → HARDWARE PARAMETERS:
SafeLINC FPII MAC Address.....:
00:08:BD:FF:FF:25
SafeLINC FPII NVRAM Data Size....: 15423 bytes
```

Figure 27. Display of MAC Address

2. Record the MAC address in the appropriate section of the MIS/IT Configuration Worksheet provided at the rear of the publication. The address is needed by the MIS/IT Department to configure the SafeLINC FPII properly on the network. Alternately, the MAC address is printed on a label located near the SafeLINC FPII's P12 connector.
3. Contact your MIS or IT administrator to have him or her complete the remainder of the MIS/IT Configuration Worksheet.
4. When you have completed the worksheet, return to your PC with your configured Hyperterm program or equivalent. Repeat Step 1 to start the boot procedure if you are not already at the prompt.
 - If you press Enter within five seconds (default), the Boot Menu (Figure 28) appears.

Note: Unconfigured systems automatically boot into the SafeLINC FPII Boot Menu.

```
SafeLINC FPII Boot Menu
=====
Choose an option below by pressing a key and then <Enter>:
<N> = Configure the SafeLINC FPII Subnet Mask
<G> = Configure the SafeLINC FPII Gateway
<I> = Configure the SafeLINC FPII Static IP Address
<A> = Configure the SafeLINC FPII Administrator Password
<U> = Configure the SafeLINC FPII 'User 1' Account
<H> = Help on the SafeLINC FPII Boot Prompt Options
<D> = Configure the SafeLINC FPII Boot-up Delay
<L> = View the SafeLINC FPII Email Log Entries
<B> = Save Current SafeLINC FPII Configuration Changes and Reboot
<S> = Summary of All SafeLINC FPII Boot Prompt Configurables
<Q> = Quit Without Making Changes and Re-Boot SafeLINC FPII
<E> = Erase SafeLINC FPII NVRAM and Restore Factory Default
Settings

Cmd:
```

Figure 28. Display of Boot Menu

Using the Boot Menu, *Continued*

Entering Data from the MIS/IT Configuration Worksheet

- Choose from the list of commands in Table 6 to configure the SafeLINC FPII. Use your MIS/IT Configuration Worksheet as a guide when entering the data.

Table 6. Boot Menu Commands

Command	Keystroke	Action
Configure Subnet Mask	N [ENTER]	Enter IP address (for example, 120.3.11.87 or 120.134.156.238).
Configure Gateway	G [ENTER]	
Configure Static IP Address	I [ENTER]	
Configure SafeLINC FPII Administrator Password Important: Choose a password that differs from any of the host FACP access level passwords.	A [ENTER]	Enter a password without spaces (6-20 characters long). Important: The password is case-sensitive.
Configure 'User 1' Account	U [ENTER]	Enter the username and password without spaces for User 1 (with administrative privileges), 6-20 characters each. Important: The username and password are case-sensitive.
Help on SafeLINC FPII Boot Prompt Options	H [ENTER]	For information about each setting, type one of the keystrokes from the Keystroke column. Type [ENTER] by itself to exit Help mode.
Boot-up Delay	D [ENTER]	Enter number of seconds, from 2 to xx, during which a key can be pressed during boot-up to change the configuration.
View the SafeLINC Email Log Entries	L [ENTER]	The contents of the email log entries sent by SafeLINC FPII are displayed.
Save Current Configuration Changes and Reboot	B [ENTER]	Configuration is saved and SafeLINC FPII reboots.
Summary of All Boot Prompt Configurables and MAC Address	S [ENTER]	All configurable boot prompt information is returned.
Quit Without Making Changes and Reboot	Q [ENTER]	Configuration is cleared and SafeLINC FPII reboots without saving the modified parameters.
Erase NVRAM But Leave MAC Address Unchanged	E [ENTER]	Entire contents of NVRAM are erased but MAC address remains intact. Configurables are restored to factory defaults. To facilitate reprogramming, press <S> for a summary of the configurables to copy down before issuing the <E> command.

Continued on next page

Using the Boot Menu, *Continued*

Entering Data from the MIS/IT Configuration Worksheet

6. After you type <S> and press [ENTER], the screen displays the following:

```
Summary of Configurables
=====
SafeLINC FPII MAC Address.....: 00:08:BD:FF:FF:1C (Not user configurable)
SafeLINC FPII Static IP Address...: 10.26.3.194
SafeLINC FPII Subnet Mask.....: 255.255.0.0
SafeLINC FPII Default Gateway.....: 10.26.1.254
SafeLINC FPII Admin Password.....: password
SafeLINC FPII 'User 1' Username...: SafeLINC_Customer
SafeLINC FPII 'User 1' Password...: password
SafeLINC FPII Boot-up delay.....: 5 seconds
```

This information stays on-screen for the duration of the Boot-up Delay period. During this period, you may press any key to further modify the settings. If you don't press a key, the system will continue to boot.

7. When you have verified that the settings are correct, type and press [ENTER] to store the configuration into non-volatile memory and reboot the SafeLINC FPII. If you didn't make any changes, type <Q> and press [ENTER] to quit without saving any modifications and the SafeLINC FPII reboots. (The SafeLINC FPII takes several minutes to boot into operation.) When normal boot-up of the SafeLINC FPII occurs, the following is displayed:

```
SafeLINC Fire Panel Internet Interface (FPII) Boot
Procedure in Progress:
SafeLINC FPII System Firmware Revision 2.00.19

SafeLINC FPII Static IP Address...: 10.26.3.194
SafeLINC FPII Subnet Mask.....: 255.255.0.0
SafeLINC FPII Default Gateway.....: 10.26.1.254

HARDWARE PARAMETERS:
SafeLINC FPII MAC Address.....:
00:08:BD:FF:FF:25
SafeLINC FPII NVRAM Data Size....: 15423 bytes
```

Notes:

- The SafeLINC FPII automatically reboots after 10 minutes of detected non-activity on the boot prompt. Any changes that you made, but did not save, are lost when the timeout occurs. The SafeLINC FPII attempts to boot into successful operation only when you specify and save all parameters.
- You must complete all parameters before the SafeLINC FPII attempts a complete boot procedure. If parameters are missing, then the SafeLINC FPII automatically goes to the boot prompt so that you can finalize the required configuration parameters.

The SafeLINC FPII is operational once you observe the message:

```
*****
The SafeLINC Fire Panel Internet Interface (FPII) is now ready for use.
*****
```

You may access the SafeLINC FPII using the assigned DNS name provided by your MIS/IT department. Refer to your MIS/IT worksheet as needed.

Starting Up the SafeLINC FPII

Logging In as an Administrator

- To start the SafeLINC FPII software and access the SafeLINC FPII, point your web browser to the assigned DNS name that's recorded on the MIS/IT Configuration Worksheet. For example, if your DNS name is `fp.ii.your_domain.com`, then point your web browser to http://fp.ii.your_domain.com/ to access the SafeLINC FPII homepage.

Note: You may need to adjust your proxy settings in your web browser depending on how your MIS/IT Department has configured the network. Because it's difficult to predict all possible configurations, consult with your MIS/IT Department on how to make adjustments to these settings. However, if your network uses a proxy server, you must configure your web browser to bypass the proxy server for local addresses.

- On the Primary Login dialog, enter your username and password (User 1 account information) from the MIS/IT Configuration Worksheet. Use the Reset button to clear the fields if necessary. The administrator (User 1) can only perform this login initially.

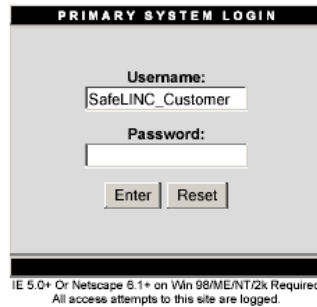


Figure 29. The Primary Login Box

- When the Home Page appears, enter the administrator password (as defined in the boot-up configuration) into the Administration Login field at the top of the screen.



Figure 30. The Home Page

The Home Page

Overview

Once you log in, the Home Page comes up, along with the standard SafeLINC FPII menus and buttons.

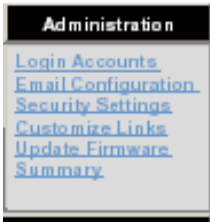
The Home Page

The SafeLINC FPII Home Page is the first page users see upon logging into the system. It consists of the following:

- Title information entered on the Customize Links screen (first appearance yields blank information due to lack of configuration)
 - Summary of panel information
 - Summary of all users designated as Administrators
 - System Menus
 - Administration Login
-

The Administration Menu

For users who have entered an Administrative password into the Administration Login field, you now have access to the functions listed in the Administration menu on the top right side of the screen. The Administration menu contains the following options:



Login Accounts. Gives the administrator access to all accounts. Accounts can be configured, edited, and deleted on this screen. Refer to “Configuring User Accounts.”

Email Configuration. Lets the administrator set up the SafeLINC email functionality and customize event messages. Refer to “Email Configuration.”

Security Settings. Lets the administrator configure lockout delay, number of login retries, logout duration, address blocking, and more. Refer to “Security Settings.”

Customize Links. Contains fields that correspond to the links and information on the Home Page. Refer to “The Home Page and Custom Links.”

Update Firmware. Allows the administrator to update SafeLINC FPII firmware. Refer to “Updating Firmware.”

Summary. Shows a general system summary. Refer to “The Summary Screen.”

Login Accounts

Overview

This section describes what you are able to do from the Login Accounts page.

To set up or edit a user account, or to change the administrator password, click the Login Accounts link on the Administration menu. Then follow the instructions in the sections below.

Setting Up a New User Account

To create a new user account,

1. Click the Add User button near the middle of the Login Accounts screen.
2. Enter the basic user information into the Account Configuration fields.
 - Username and password are case-sensitive and cannot contain any spaces.
 - Username and password must be 6 to 20 characters long.
3. Use the drop-down list boxes in the Account Maintenance section to complete the user setup.
 - Administrative privileges can only be granted or revoked by User 1.
 - A disabled account cannot be used until an administrator enables it again.
4. Enter a custom message (if necessary). Custom messages can be up to 180 characters long.
5. Click the Update button. You are now returned to the Login Accounts screen.

Notes:

- The SafeLINC FPII can support a maximum of 20 user accounts.
- A verification dialog appears if you choose to delete an account. You cannot recover an account once it is deleted.
- You must configure an email address to verify email configuration settings. An email address is required to receive event notification. This email address can be any valid internet email address or a distribution list configured by your MIS/IT Department.
- You should print a summary of accounts because this information is not available for review at the boot prompt.

The Account Information section of the Login Accounts screen now reflects the user settings. A sample account is shown below.

Summary of Configured User Accounts

User 1	Account Access: <input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled	Administrator Access: <input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Name: SafelINC_Customer	Designated Emergency Contact: <input checked="" type="checkbox"/> Fire <input checked="" type="checkbox"/> Pri2 <input checked="" type="checkbox"/> Supv <input checked="" type="checkbox"/> Trbl	
Email: Customer@customer-site.com	Logs, Reports, & Email Frequency: <input checked="" type="checkbox"/> Weekly <input type="checkbox"/> Bi-weekly <input type="checkbox"/> Monthly	
Primary: (555) 555-5555	Email Event Notification: <input checked="" type="checkbox"/> Fire <input checked="" type="checkbox"/> Pri2 <input checked="" type="checkbox"/> Supv <input checked="" type="checkbox"/> Trbl	<input checked="" type="checkbox"/> Alarm <input checked="" type="checkbox"/> Trouble <input checked="" type="checkbox"/> Service <input checked="" type="checkbox"/> Status
Alternate:	<input checked="" type="checkbox"/> SafeLINC Security Violations	Detectors: <input checked="" type="checkbox"/> Dirty <input checked="" type="checkbox"/> Excessively Dirty
Cellular:		
Pager:		
Message: I will be on vacation next week.		

Figure 31. User Information

Adding/Editing a User Account

To edit a user account, click the name of the account you want to edit to bring up the Revise Existing User screen. To add a user, click on the Add User icon.

Login Accounts, *Continued*

Changing the Administrator Password

The administrator (User 1) has exclusive control over the administrator password. To change the administrator password, follow the prompts in the *Change Administrator's Password* section of the screen. Note that passwords must be between 6 and 20 characters long and cannot contain any spaces. Usernames and passwords are case-sensitive.

Note: The Administrator's password is shared among multiple designated Administrators.

IMPORTANT: For maximum security, change the Administrator's password often, especially when a user is no longer an employee.

HINT: If you forget the administrator's password or login information for the User 1 account, you can reset/override these options via the boot prompt on the Diagnostic Port. You should contact your local Simplex product representative to assist you in making this change.

Email Configuration

Overview

This section describes how to set up the SafeLINC FPII for sending email.

To set up the system for sending email, click the Email Configuration item on the Administration menu. Then follow the instructions below.

Configuring SafeLINC FPII Email

To configure the system for email:

1. Use the MIS/IT Configuration Worksheet to enter information into the configuration fields (see Figure 32).

SMTP Mail Server IP Address:	<input type="text" value="10.1.24.217"/>	Port:	<input type="text" value="25"/>
SafeLINC FPII Email Account Address:	<input type="text" value="customer@customer-site.com"/>		

Note: The SMTP Port is not configurable and is fixed at 25.

Figure 32. Applicable Portion of Configuration Program

2. Click the Send Test Email hotlink to test your configuration. Click Send Test Email on the verification dialog. Check the mail account for where the email address receives mail to verify that you received the test email. You may need to click on Send/Receive in your email client to get the new email.

Notes:

- Your browser may display any problems with the SafeLINC FPII sending the test email message. You may also view the messages in the Diagnostic Port.
- You also can use the email log feature under the system menu to help you in configuring email properly.

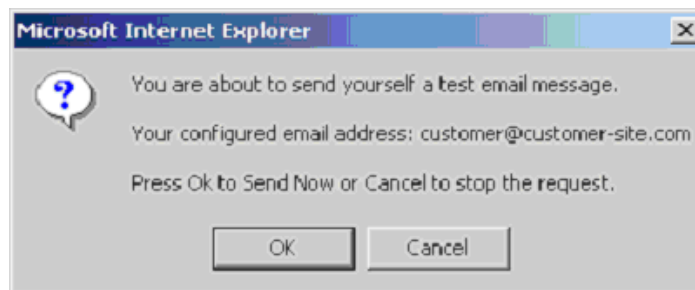


Figure 33. Test Email Box

Email Configuration, *Continued*

Disabling Outgoing Email

When servicing the host FACP, you may choose to globally disable outgoing SafeLINC FPII email to halt unnecessary event email traffic. Click on the Disabled radio button (see figure below) to disable outgoing SafeLINC FPII email. While email is disabled, a reminder email is sent to all SafeLINC FPII administrators once every 24 hours (around 5:30 a.m. daily).

Disable Outgoing Email

When servicing the host FACP, you may want to globally disable outgoing SafeLINC FPII email to prevent unnecessary event email traffic. A reminder email shall be sent to all SafeLINC FPII configured administrators once every 24 hours around 5:30 am daily until the outgoing SafeLINC FPII email is re-enabled.

The Email Configuration must be operational for this feature to have any affect on the SafeLINC FPII.

Outgoing SafeLINC FPII Email is Currently: Enabled Disabled

[Update](#)

Figure 34. Disabling Outgoing Email

Configuring the Email Health Status Check

To configure the email health status check, you need to enter the time interval (in minutes) to specify how minutes will pass before the SafeLINC FPII checks the configured email server again for proper email connectivity. Clicking the Update button applies your setting. See the figure below.

Email Health Status Check

The SafeLINC FPII periodically checks the configured email server specified above to ensure that the SafeLINC FPII email capability is properly maintained. Should the SafeLINC FPII fail to connect to the configured email server, then the status shall be reported under System Summary. Specify the checking interval below.

Email Health Status Check Interval: min (5-30 minutes; default = 15 minutes)

Figure 35. Email Health Status Check

Customizing Event Messages

To customize the messages that will be sent each time an event occurs:

1. In the Event Message Customization section of the Email Configuration screen, click the desired message type in the Edit Message column as shown in Figure 36.
 - The Customize Fire Event Message dialog comes up.

Click the desired link to change the message configuration for that link.

Edit Message	View Message	Send Test Event Email
Fire	<input checked="" type="checkbox"/> Default <input type="checkbox"/> Custom	Test Fire Event Email
Priority2	<input checked="" type="checkbox"/> Default <input type="checkbox"/> Custom	Test Priority2 Event Email
Supervisory	<input checked="" type="checkbox"/> Default <input type="checkbox"/> Custom	Test Supervisory Event Email
Trouble	<input checked="" type="checkbox"/> Default <input type="checkbox"/> Custom	Test Trouble Event Email
SafeLINC FPII Security	<input checked="" type="checkbox"/> Default <input type="checkbox"/> Custom	Test SafeLINC FPII Security Event Email

Figure 36. Message Table

2. Use the “System shall use:” drop-down list to select either a custom or default message for all messages of this event type. If you select Custom Message, enter the message into the text box. Messages can be up to 480 characters long.
3. Click the Update button.
 - Custom messages are appended to the default messages.
 - Custom messages may contain special instructions to other SafeLINC FPII users.

Email Configuration, *Continued*

Understanding Email Event Notification

Since email event notification operates differently according to the event message being sent, a description of each event notification is given below.

Fire and Priority2 - For event types FIRE and PRIORITY2, one email is sent immediately to all actively configured users who've elected to receive FIRE and/or PRIORITY2 event email. This message always takes priority over all other system events.

Supervisory - When a Supervisory event occurs, a 30-second timer in the SafeLINC FPII begins. During this time interval, all supervisory events are collected and combined into a single email message. When the 30-second timer expires, the SafeLINC FPII completes the email message by sending it to all actively configured users who have elected to receive supervisory event email. Supervisory event email is only superseded by Fire and Priority2 events, which take precedence. The process is repeated until no more supervisory events are detected.

Trouble - When a Trouble event occurs, a 30-second timer in the SafeLINC FPII begins. During this time interval, all trouble events are collected and combined into a single email message. When the 30-second timer expires, the SafeLINC FPII completes the email message by sending it to all actively configured users who have elected to receive trouble event email. Trouble event email is only superseded by Fire and Priority2 events, which take precedence. The process is repeated until no more trouble events are detected.

SafeLINC FPII Security Violations - Sent to all configured SafeLINC FPII administrators who've elected to receive these event types, this message is sent out immediately upon detecting the event (like a Fire or Priority2 event). A Security Violation message is only superseded by Fire and Priority2 events, which take precedence. If the SafeLINC FPII is in the locked state as a result of a security violation, it will unlock for any of the four events: Fire, Priority2, Supervisory, and Trouble. This feature permits the configured users to immediately gain access to the system if needed.

Security Settings

Overview

The administrator can configure security settings, such as lockout delay, number of retries for logging in, and IP address blocking.

To customize the security settings, click the Security Settings item on the Administration menu. Then follow the instructions below.

Description of Security Settings

Enter or select the required security settings.

Automatic Lockout Delay. The Lockout Delay period is the amount of time the SafeLINC FPII can remain idle before logging the user out and returning the host FACP to the lowest access level (3-30 minutes; default is 10 minutes).

Note: The SafeLINC FPII returns to the host FACP at the lowest login level after 10 minutes of inactivity, or when the user logs out or is automatically logged out.

Login Retries. Specify the number of incorrect logins (1-20 times; default is 3 times) allowed before the SafeLINC FPII enters lockout. (All users will be unable to log in during lockout.)

SafeLINC FPII Lockout Duration. Specify the amount of time each lockout will last (0-24 hours; default is 1 hour).

Note: If an event occurs while the SafeLINC FPII is in the lockout state, the lockout duration expires upon detecting the event that allows users to log in.

Local Configuration Options. These options specify whether you must configure the SafeLINC FPII on the same sub-domain on which the SafeLINC FPII resides, or on any domain. For example, if the SafeLINC FPII is at 192.168.0.1 and you are accessing the SafeLINC FPII from 193.168.0.2 with the “Local” option enabled, you would not be able to modify the IP blocking features. The same rule applies to Email and User Account options. To disable the “Local” option, you must access the SafeLINC FPII on the same sub-domain (for example: 192.168.0.4 is on the same sub-domain as 192.168.0.1).

Configure IP blocking locally.

Configure email accounts locally.

Configure user accounts locally.

Network Status Check. Specify a time interval (in minutes) for when the SafeLINC FPII checks for the presence of its configured network gateway. (With 30 minutes being the default interval, you can change the interval anywhere from 0 minutes to 4 hours. Entering 0 minutes disables this feature.)

Although this feature does not guarantee that the entire network is operational, it does confirm that the SafeLINC FPII can communicate on the network.

Continued on next page

Security Settings, Continued

Description of Security Settings

IP Address Blocking. The SafeLINC FPII provides the ability to allow users by IP address or deny users by IP address. Select which method you prefer by using the radial button shown below.

IP Address Blocking

Use IP address blocking to lock out undesired users. IP address can be either a fully qualified domain, or a wildcard entry (e.g., 192.168.0.1;10.10.*). Use semicolons to separate entries.

The SafeLINC FPII has detected your IP Address as 10.26.3.194. To use this feature effectively, you must ensure that you are bypassing local addresses when using a proxy server. Consult with your MIS/IT department for further details on how to configure your browser properly.

IP Address Blocking is: Enabled Disabled

Allow Access or Deny Access to All Except: Characters Remaining

180 Characters Maximum

Figure 37. IP Address Blocking

Allow Access to All (IP Addresses) But - Enter one or more IP addresses that will not be able to successfully access the SafeLINC FPII. Separate each address with a semicolon. You can use a wildcard (asterisk [*] is a wildcard that denotes a range of IP address numbers). For example, 192.168.0.* will only deny access to IP Addresses 192.168.0.0 through 192.168.0.255.

Deny Access to All (IP Addresses) But - Enter one or more IP addresses that will be able to successfully access the SafeLINC FPII. Separate each address with a semicolon. You can use a wildcard (asterisk [*] is a wildcard that denotes a range of IP address numbers). For example, 192.168.0.* will only allow access to IP addresses 192.168.0.0 through 192.168.0.255.

Use this feature to lock out undesired and problematic users.

When you have completed the settings, click the Update button at the bottom of the screen. If you wish to reset the screen to the default settings, click the Reset button.

Note: *Allow* and *Deny* are mutually exclusive (only one or the other can be used at one time).

Customize Links

Setting Up the Home and User Links Pages

Any active Administrator can set up the Home page (the page that comes up when you click the Home link on the right side of the screen) and the User Links page (which comes up when you click User Links in the System Menu). The Home page and the Links page are both configurable from the Custom Links screen.

To set up the Home and User Links pages, click the Customize Links item. Then follow the instructions on the screen.

The panel location description appears in the black bar at the top of the screen.

The title fields are typically used to describe the building or facility in which the panel is installed.

Enter an address to appear as a link on the User Links page.

Enter a description to appear below the link.

Customer's Building Good Morning, SafeLINC_Customer Home | Log Out | Help | About

System
[System Cards](#)
[View Point Data](#)
[System Summary](#)
[Account Settings](#)
[User Links](#)
[Email Log](#)

SafeLINC FPII : Administration : Custom Links Configuration

Customize Your Title Page

You can customize the title of the SafeLINC FPII homepage using the three lines provided below. Each line is limited to 45 characters maximum.

Line 1:

Line 2:

Line 3:

Specify Your Panel Location

Using the field provided below, you can specify the location of the FACP where the SafeLINC FPII card is installed. The location is limited to 45 characters maximum.

Location:

Custom Links

Add your custom hypertext links below. This feature allows you to provide customized hypertext links to important sites or to websites that can provide detailed instructions on what to do should an event occur.

Link 1: 50 Characters Maximum

As the industry's premier provider of fire and life safety, SimplexGrinnell is dedicated to meeting the needs of customers. Characters Remaining

180 Characters Maximum

Link 2: 50 Characters Maximum

Characters Remaining

180 Characters Maximum

Figure 38. Custom Links Screen

When you are done entering the information, click the Update button at the bottom of the screen.

Updating Firmware

Overview

The administrator has the capability of updating SafeLINC FPII system firmware. This section covers this capability.

Firmware Update Procedure

Note: To minimize any chance of error, reboot the system before performing this procedure. For Rev. B and later SafeLINC FPII cards, you may press SW1 on the SafeLINC FPII to reboot the system.

Be sure to read this procedure carefully before you attempt to update the firmware in the SafeLINC FPII. Failure to do so may render the SafeLINC FPII inoperable. To avoid any mistakes, verify your entries carefully before pressing the Enter key.

IMPORTANT: Only experienced administrators or your local Simplex product representatives should use the Update SafeLINC FPII screen. Improper use of the Update SafeLINC FPII screen may render the SafeLINC FPII inoperable.

1. Log in as the User 1 Administrator on the web site.
2. When the menu returns, click the Updating Firmware link on the right side of the screen.
3. Now click the Start FTP Server. You should obtain the screen shown in Figure 39.

Notes:

- Once the FTP Server is started, only User 1 can log in – all others are denied access.
- Throughout the procedure, observe the Diagnostic Port (if available) for status information.

Note: The SafeLINC FPII reboots after 10 minutes of inactivity once the FTP Server is started. The system also reboots upon successful update of the SafeLINC FPII firmware.

HINT: If you accidentally start the FTP server, don't do anything and the SafeLINC FPII reboots after 10 minutes of FTP inactivity.

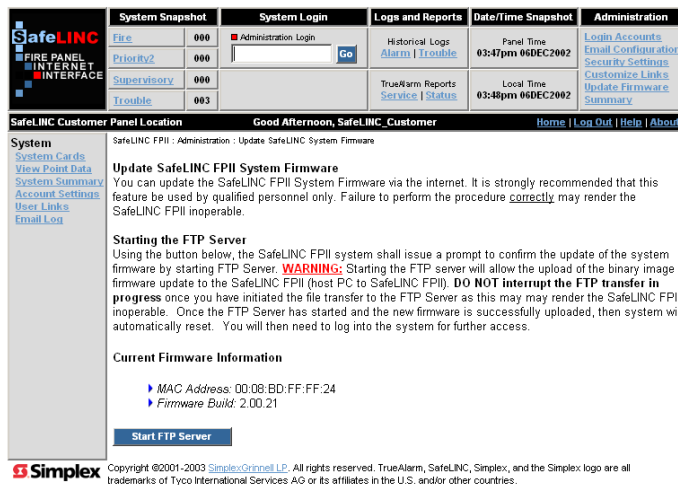


Figure 39. Start FTP Server Verification Screen

Continued on next page

Updating Firmware, *Continued*

Firmware Update Procedure

4. In the dialog box, click OK to start the FTP Server. Observe the diagnostics port using your favorite Terminal program to see that a message appears about starting the FTP server (Starting FTP Server). Refer to “Connecting a PC to the SafeLINC FPII Diagnostic & Configuration Port” section earlier in this publication if you require information on setting up the terminal program.
5. Now open up a DOS window. You will use DOS FTP to upload the new image.

Note: You must use DOS FTP to perform this procedure properly. Do not attempt to use another FTP program or your update procedure will fail.

6. Navigate to the same directory as the safelinc.obf image. The image should be in its own directory to minimize the chance of errors.
7. At the DOS prompt, type *ftp 10.26.3.194* (substituting the IP address of your SafeLINC FPII card for the IP address example of 10.26.3.194) and press <ENTER>. Figure 40 shows a transcript of the DOS window from an update performed on a typical SafeLINC FPII card.

```
C:\CUSTOMER\DESKTOP>ftp fpII.simplexnet.com
Connected to fpII.simplexnet.com.
220 NET+ARM FTP Server 1.0 ready.
User (fpII.simplexnet.com:(none)): SafeLINC_Customer
331 User SafeLINC_Customer OK, send password.
Password:
230 Password OK.
ftp> bin
200 Type set to I.
ftp> put safelinc.obf
200 PORT command Ok.
150 About to open data connection.
226 Transfer complete
ftp: 485476 bytes sent in 0.73Seconds 663.22Kbytes/sec.
ftp> bye
221 Goodbye.
C:\CUSTOMER\DESKTOP>
```

Figure 40. Typical DOS Window Showing FTP Transfer of SafeLINC FPII Upgrade Firmware

8. As assigned by the SafeLINC system administrator, type in the user name (case sensitive) and press <ENTER> before typing in the password (case sensitive) and pressing <ENTER>.

Note: Only User 1 can log in and perform this update. All others are denied access.

9. At the prompt, type *bin* and press <ENTER>. This command sets the file transfer mode to binary.
10. At the prompt, type *put safelinc.obf* and press <ENTER>. Since this step is very important, make sure that you've typed it in correctly before pressing <ENTER>. The file transfer begins. Observe the dialog window for status information.
11. Back in the DOS window, you see the ftp prompt return. Type in *bye* then press <ENTER>. This command closes the ftp session with the SafeLINC FPII.
12. In the dialog window, you see *Download complete, rebooting...*
 - The SafeLINC FPII Update Procedure is now complete.

Summary

Viewing a Summary of Administrative Changes

For a summary of all administrative changes you've made, click the Summary link on the Administration menu. The following sections come up as shown in Figure 41.

Customer's Building Good Morning, SafeLINC_Customer Home | Log Out | Help | About

SafeLINC FPII Administration Summary

System
[System Cards](#)
[View Point Data](#)
[System Summary](#)
[Account Settings](#)
[User Links](#)
[Email Log](#)

SafeLINC FPII Administrative Summary
Below is a report summary of all the items configurable in the SafeLINC FPII Administration Area. This report should be printed and stored in a safe place for your records.

Configured Login Accounts
Please visit [Login Accounts](#) to View the User Account Summary

Email Configuration
SMTP Mail Server IP Address: 10.1.24.217
SMTP Mail Server Port Number: 25
Email Account Username: customer@customer-site.com
Email Health Status Check Interval: 15 min

Event Message Customization - Message Status
Fire Events: Default
Priority2 Events: Default
Supervisory Events: Default
Trouble Events: Default
SafeLINC FPII Security Events: Default

Security Settings
Automatic logout delay: 10 min
Login retries before lockout: 3 times
User lockout duration: 1 hour(s)
Configure IP blocking locally: No
Configure email accounts locally: No
Configure user accounts locally: No
Network Status Check Interval: 30 min
IP Address Blocking: Disabled
IP Address Blocking Entries

Custom Links
Title
Line 1: Customer Name
Line 2: Customer Location
Line 3: Anytown, USA
Links
Link 1: <http://www.simplexgrinnell.com/>
Text 1: As the industry's premier provider of fire and life safety, SimplexGrinnell is dedicated to meeting the needs of customers.

Boot Prompt Configurables
SafeLINC FPII MAC Address: 00:08:BD:FF:FF:1C (Not user configurable)
SafeLINC FPII IP Address: 10.26.3.194
SafeLINC FPII Subnet Mask: 255.255.0.0
SafeLINC FPII Default Gateway: 10.26.1.254
SafeLINC FPII Administrator Password: (Not Shown)
SafeLINC FPII 'User 1' Username: SafeLINC_Customer
SafeLINC FPII 'User 1' Password: (Not Shown)
SafeLINC FPII Boot-up Delay: 5 sec

SafeLINC FPII Administration Summary Report Completed 11:09:02 am WED 7-AUG-02

Figure 41. The Administrator Summary Screen

Login Accounts. Refers you to Login Accounts screen for in-depth user account information.

Email Configuration. Lists email server IP address, port number, and account username.

Event Message Customization – Message Status. Lists whether the messages are custom or default.

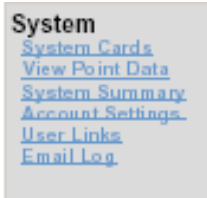
Security Settings. Lists the settings made on the Security Settings screen.

Custom Links. Lists the contents of the Home Page, complete with hypertext custom links.

Boot Prompt Configurables. Lists the contents of the configurable items from the boot prompt. The MAC address is also displayed here, too. No passwords are shown.

General Operations

The System Menu



The System menu is always on the left side of the screen, regardless of the page you are on. The System menu contains the following options:

System Cards. Lists all the cards in the system. Refer to the section “Viewing System, Card, and Point Reports.”

View Point Data. Lists all the points in the system. Refer to the section “Viewing System, Card, and Point Reports.”

System Summary. Lists some basic SafeLINC FPII and panel information. Refer to the section “Viewing System, Card, and Point Reports.”

Account Settings. Gives the user access to his or her account settings (password, email, etc.).

User Links. Displays links to sites entered into the Custom Links page.

Email Log. Displays a log of the last 25 emails sent by the SafeLINC FPII. This log is primarily used as a diagnostic tool during email configuration. It is also accessible via the boot prompt.

Checking the System Status

You can always tell whether there is an urgent condition by looking at the numbers under the System Snapshot section at the top of the screen.



System Snapshot	
Fire	002
Priority2	000
Supervisory	000
Trouble	019

← This example shows 2 Fire events, no Priority 2 or Supervisory events, and 19 Troubles.

Figure 42. System Snapshot

Click on any one of the four links for detailed information. The screen will display important information about the event, including the point address, the custom point description, how the event was triggered, and whether the event has been acknowledged. At the panel, all designated emergency contacts are also shown, along with email, phone, and pager listings.

Notes:

- All users that are designated as emergency contacts for the event selected will be shown following the display of specific event information.
- The events counts are not dynamically updated. They are updated the next time a web page is requested from the SafeLINC FPII. Think of them as snapshots of the panel at the time the web page was accessed.

HINT: To update the event counts, click any of the four event icons shown in Figure 42.

Continued on next page

General Operations, *Continued*

Checking the System Status

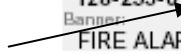
SafeLINC FPII : System Event Snapshot : Fire Event(s)

Active Fire Event(s)

A snapshot of the active fire events are listed for your system below. Click on the hypertext custom label to obtain detailed information about the point shown. To refresh the active Fire Event list, click on the Fire hypertext link located under System Snapshot above.

FIRE	
Point Address & Custom Label:	Needs Ack?
128-233-0 REMINDER - FIRE ALARM(S) EXIST IN SYSTEM	YES
Banner:	Status:
FIRE ALARM POINT	FIRE
Point Address & Custom Label:	Needs Ack?
130-0-0 FRONT PANEL FIRE ALARM PSEUDO POINT	NO
Banner:	Status:
FIRE ALARM POINT	FIRE

Click on the Point Description for detailed information on the event.



All users designated as emergency contacts for this event type are listed.

Emergency Contact(s)

- Name: SafeLINC_Customer
- Email: Customer@customer-site.com
- Primary Tel: (555) 555-5555
- Message: I will be on vacation next week.

Click the Email field to send an email to the emergency contact.



Figure 43. Event Screen

Viewing System, Card, and Point Reports

Overview

The SafeLINC FPII web pages allow you to view general and specific system data. This section describes how to bring up summary data for the host panel, as well as individual cards and points.

Viewing TrueAlarm Service Reports

To view TrueAlarm Service reports, select Service under TrueAlarm Reports in the Logs and Reports section at the top of the screen. TrueAlarm Service reports display the device number and custom label for each point in a channel, as well as:

Alarm At. The percentage of a value/ number of units of a value (for example, smoke on a smoke detector) that the device needs to sense to go into alarm.

Average Value. The number of units of a value (for example, smoke on a smoke detector) that the device currently detects on average.

Current/% Alarm. The current number of units of a value/ percentage of a value (for example, smoke on a smoke detector) that the device currently senses.

Peak/% Alarm. The highest number of units of a value/ percentage of a value (for example, smoke on a smoke detector) that the device has sensed.

Current State. Shows the message the device is sending to the panel (Normal, Alarm, Trouble, Supervisory, No Response, etc.).

Email This Report. Allows you to email the displayed report. The size of the report may require the system to send multiple email messages. When the report is requested, it will be sent via email to the user who is currently logged into the system.

Viewing TrueAlarm Status Reports

To view TrueAlarm Status reports, select Status under TrueAlarm Reports in the Logs and Reports section at the top of the screen. TrueAlarm Status reports display the zone name and custom label for each point in a channel, as well as:

Current Sensitivity. The percentage of a value (for example, smoke on a smoke detector) that must be detected by the device to go into alarm.

Device Status. Shows the message the device is sending to the panel (Normal, Alarm, Trouble, Supervisory, No Response, etc.).

Almost Dirty. Displays *YES* when the average device sensitivity is close to alarm levels. You must turn on P132 for this field to display data at the host FACP. Turning on P132 causes all Almost Dirty detectors to display a trouble at the panel.

Email This Report. Allows you to email the displayed report. The size of the report may require the system to send multiple email messages. When the report is requested, it will be sent via email to the user who is currently logged into the system.

Viewing Point Summaries

To find information about a specific point, click the View Point Data item on the System menu.

A screen comes up, showing the expected point number formats for each type of point. Below the list of expected point formats is a list of card addresses and corresponding card types. Below that are a drop-down list and an empty number field.

Use the drop-down list to select the type of point you want a report on. Next, enter the point number, using the list of expected point number formats as a guide. Click Update to bring up the report.

The point report that comes up is identical to what you see when you click the point as a hyperlink. Refer to "Report Items" under "Basic Reports," later in this publication.

Viewing System, Card, and Point Reports, *Continued*

Viewing Card Summaries

To find information about a specific card, click the System Cards item on the System menu.

The System Cards screen comes up, showing the number and description for each card in the system.

Click on the hyperlink for a card to bring up a screen that lists every sub-point for that card, as well as each sub-point's status if applicable.

Viewing the SafeLINC FPII/Host Panel Summary

For information about the SafeLINC FPII module and its host panel, click the System Summary item on the System menu.

The System Summary report includes the following information for those systems supporting these features:

Host FACP – System Revision and Job Build Information. Lists the system revision and CFG format. Also lists the name, date, revision, and activation for the job build.

Host FACP – Serial Number Information. Lists the serial number for the host FACP as well as the firmware revisions for the System Power Supply and IDNet.

Host FACP – SafeLINC FPII Communication Status. Lists the status of the RUI/4100 Slave Communications.

SafeLINC FPII – General Information. Lists the IP and MAC addresses as well as information on the Job and Firmware builds.

SafeLINC FPII – System Status. Lists statuses for the network, email, and FTP server.

Viewing Alarm and Trouble Logs

You can view alarm and trouble logs from the SafeLINC FPII web pages.

- To view a log of past alarms, click Alarm under Historical Logs in the Logs and Reports section at the top of the screen.
- To view a log of past troubles, click Trouble under Historical Logs in the Logs and Reports section at the top of the screen.

Each log includes the time and location for each event that occurred.

There is also an “Email Report” button that allows you to send the displayed log via email. The size of the log may require the system to send multiple email messages. When the report is requested, it will be sent via email to the user who is currently logged into the system.

Basic Reports

Overview

When you click on a Custom Label for any event, a screen comes up that summarizes the address corresponding to that label. This section explains the details of the summary report.

Report Items

Here are some of the items that may be displayed whenever a system point is shown as a hyperlink.

Current Device. Displays whether the device is seen correctly by the system.

Device. The device status (Alarm, Trouble, Supervisory, No Answer, etc.).

Test State. Shows whether the device is self-testing, and the results of a self-test.

Present Sensitivity Selected. The percentage of a value (for example, smoke on a smoke detector) that must be detected by the device to go into alarm.

Average Value. The number of units of a value (for example, smoke on a smoke detector) that the device currently detects on average.

Alarm Level. The number of units of a value (for example, smoke on a smoke detector) that the device needs to sense to go into alarm.

Value. The current number of units of a value (for example, smoke on a smoke detector) that the device is detecting.

Peak. The highest number of units of a value (for example, smoke on a smoke detector) that the device has detected in the past.

Trouble Threshold. The value that the device needs to cause the display of a trouble message.

Enabled State. Shows whether the device is enabled or disabled. Devices may be enabled or disabled via the SafeLINC FPII.

Unverified. System points that are not returning a value.

MIS/IT Configuration Worksheet

SafeLINC Fire Panel Internet Interface MIS/IT Configuration Worksheet

About the SafeLINC Fire Panel Internet Interface

The SafeLINC Fire Panel Internet Interface (FPII) is a module that mounts internally to a fire alarm control panel (FACP) located on your premises to provide the ability to access FACP information using the Internet Explorer 5.0+ web browser. The SafeLINC FPII has the ability to send FACP event notification via email and requires a SMTP email account to function properly. To interface the FACP to your Internet LAN, an EIA/TIA-568A CAT-5 (10/100-BaseT)-compliant Ethernet drop to the panel is required. This connection requires a standard Ethernet RJ-45 terminating connector. It is strongly recommended that the SafeLINC FPII be installed behind your network firewall to maintain maximum security for your network.

Before You Approach Your MIS/IT Department

Find the MAC address that is printed on a label located near the SafeLINC FPII's P12 connector. Carefully record this number below because your MIS/IT department will need this information to configure the SafeLINC FPII properly on your network. The format of the MAC address will look something similar to 00:08:BD:1C:48:1A. As an alternative to finding the MAC address on the label, follow the procedures in the SafeLINC FPII Installation, Setup, and Operating Instructions (Publication 579-349) to gain access to the SafeLINC FPII boot prompt. The MAC address will be displayed initially upon boot-up.

Record the FPII MAC Address: : : : : : Ex: 00:08:BD:1C:48:1A

Minimum Parameters Required to Boot SafeLINC FPII – IT/MIS Department to Complete This Section

Now you may take this worksheet to your MIS/IT department for assistance in obtaining the parameters required for the SafeLINC FPII to operate properly on your local network. The parameters requested below are the minimum requirements necessary for the FPII to boot successfully into operation. **WARNING: Do not attempt to boot the FPII using random entries; serious consequences may result. You can inadvertently affect other computers and networked devices on your network or, even worse, the Internet.**

Below are the minimum parameters for the SafeLINC FPII to successfully boot into operation on your network. Your MIS/IT department must complete this section using the MAC address that you've provided from your SafeLINC FPII above.

MIS/IT Assigned FPII Static IP Address: . . . Ex: 192.168.0.1

To configure the static IP address, type I at the FPII boot prompt. To verify your entry, type S to review a summary of all boot prompt configurables.

MIS/IT Assigned FPII Gateway: . . . Ex: 192.168.254.1

To configure the gateway, type G at the FPII boot prompt. To verify your entry, type S to review a summary of all boot prompt configurables.

MIS/IT Assigned FPII Subnet Mask: . . . Ex: 255.255.0.0

To configure the subnet mask, type N at the FPII boot prompt. To verify your entry, type S to review a summary of all boot prompt configurables.

MIS/IT Assigned FPII DNS Name: Ex: fpii.your_domain.com

The FPII DNS name is not a required boot prompt menu parameter. It is used to access the FPII and is described below.

NOTE: The DNS Name Assignment requires an entry on the DNS server that maps to the FPII Static IP address or MAC address depending on your type of server.

Additional Parameters Required for SafeLINC FPII Email Support – IT/MIS Department to Complete This Section

Below are the minimum required parameters for the SafeLINC FPII to enable email functionality. Most email server configurations do not allow email relaying for network security reasons. Therefore, the SafeLINC FPII requires a valid email account to log into and send email as required. The account should not be configured to receive email because the SafeLINC FPII lacks the functionality to do so. All incoming email on this account should be simply deleted. This account should be dedicated to the fire panel so that it can be distinguished among other email accounts.

SMTP Email Server IP Address: . . . Ex: 192.168.0.1

SMTP Email Server Port: Fixed at Port 25 (not configurable)

SMTP Email Account Address: Ex: fire_panel@customer-site.com

Continued on next page

MIS/IT Configuration Worksheet, *Continued*

SafeLINC FPII MIS/IT Configuration Worksheet, *Continued*

SafeLINC FPII Administrator's Account – SafeLINC FPII Administrator to Complete This Section

In addition to the parameters obtained above, the SafeLINC FPII requires a username and password for the first user (Administrator) before a successful boot can proceed. This is the username and password that you will use to gain access the SafeLINC FPII via the Internet. To administer the SafeLINC FPII, the SafeLINC FPII Administrator's password is also required. Keep the information in this section private and store this sheet in a secure place.

FPII User 1 Username:

Ex: John_Doe

FPII User 1 Password:

Ex: Password

To configure the 'User 1' account, type U at the FPII boot prompt. You will be first prompted to enter the username followed by the password for this account. Enter the information as it appears above. To verify your entry, type S to review a summary of all boot prompt configurables.

FPII Administrator's Password:

Ex: Admin_Pw

To configure the FPII Administrator Password, type A at the FPII boot prompt. Enter the password as it appears above. To verify your entry, type S to review a summary of all boot prompt configurables.

Once you have successfully completed this sheet with the assistance of your MIS/IT department, you will be ready to configure the SafeLINC FPII via the diagnostic port and boot prompt. Using the above parameters, return to the SafeLINC FPII boot prompt to configure the SafeLINC FPII. The Email Support parameters are not required for the boot prompt configuration but will be required once you are able to access the SafeLINC FPII via your web browser.

At the SafeLINC FPII boot prompt, select the letter option to be configured followed by a carriage return. Help is available by typing H; typing S summarizes all the parameters as they are currently configured. If you wish to extend the boot-up delay, type D and enter the value in seconds. When you have finished entering the parameters from above and have verified they are correct (using S), type B to save the options into memory and reboot the SafeLINC FPII. Your SafeLINC FPII should now be configured for use on the network.

Accessing the SafeLINC FPII for the first time on your Network

You cannot proceed with the SafeLINC FPII Email configuration until you can access the SafeLINC FPII at the assigned DNS name from above. For example, if your DNS name is: `fpii.your_domain.com` then point your web browser to: `http://fpii.your_domain.com/` to access the SafeLINC FPII homepage. You may need to adjust your proxy settings in your browser depending on how your MIS/IT department has configured the network. Because it is difficult to predict all possible configurations, please consult with your MIS/IT department on how to make adjustments to these settings. Refer back to earlier sections of Publication 579-349 for more details.

Once you can successfully access the SafeLINC FPII using your web browser, log into the SafeLINC FPII entering your username and password in the areas provided. Upon successful login, you will arrive at the homepage of the SafeLINC FPII. To access the administration area, you must use the Administrator's password in box provided at the top of the page. Enter the Administrator's password and press the carriage return. A new menu icon titled, Administration, will appear on the top right menu if the login was successful.

Next, click on the Login Accounts link and then scroll down to edit your account (the only one listed) and complete the information requested. You must provide a valid email address to test out the email configuration set-up described below. When you have finished editing your account, click Update to complete the request.

The last step is to configure the email configuration parameters in order for the SafeLINC FPII to send out email. Click on the Email Configuration link. The information provided by your MIS/IT department from above is used to complete the email configuration options. Fill in the information requested and press Update to complete the request. To verify that email is working properly, click on Send Test Email and then follow the directions. To verify that the email was sent properly, use your mail client and check the email account where you expect to receive email. This account should be the same as the email address provided in Login Accounts section. You may need to click on Send/Receive in your email client to see if you have received your email message. In addition, you may also check the email log on the SafeLINC FPII to verify that the SafeLINC FPII connected to the mail server successfully and delivered the message. To do so, locate the System menu and click the Email Log link. Review the log entries. If the SafeLINC FPII reports an error in the log, you will need to re-verify your email configuration settings on the SafeLINC FPII.

Congratulations! The SafeLINC FPII is now configured for general use. You will still need to configure some additional options and add user accounts as needed. Please refer to Publication 579-349 for how to operate the SafeLINC FPII.

579-349
Rev. H



FIRE • SECURITY • COMMUNICATIONS • WORLDWIDE SALES & SERVICE

© 2002-2011 SimplexGrinnell LP. Specifications and other information shown were current as of publication and are subject to change without notice.