SECURITY

DEVICE

INSTALLATION

MANUAL

LIGHTGARD™

Fiber-Optic Detection System

Interactive Technologies, Inc.®

LightGard

Fiber-OpticDetectionSystem

Interactive Technologies, Inc.
2266 North Second Street
North Saint Paul, MN 55109
(612) 777-2690
(612) 777-1415

ITI 1993 - Document Number 46-599-C
Issue Date May, 1993

Table of Contents

List of Figures

List of Tables

Section 1 Introduction

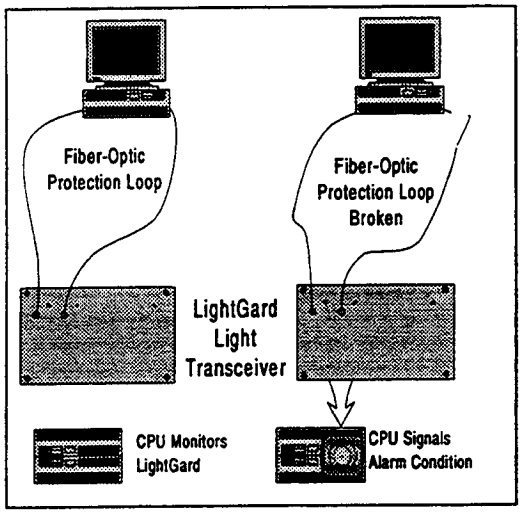

Figure 1.1 LightGard protects your assets with a fiber-optic loop

The LightGard device provides security for computers, peripherals, and other transportable equipment. A fiber-optic loop protects the equipment and must be threaded through all internal, external, and peripheral components of the equipment to be protected. If someone breaks the fiber-optic loop by attempting to remove the protected equipment, the LightGard Transceiver Module (LTM) sends an alarm signal to your control panel.

The LightGard device is in contact with your current security system's control panel either by a wireless transmitter or hardwired connection to provide 24-hour protection to selected equipment. Depending on the configuration of your system, each LTM can be used to pinpoint the exact building, room, and type of equipment that is being tampered with. Figure 1.1 illustrates how LightGard works to protect your valuable assets.

This device is available in three configurations: LightGard Wireless, which interfaces with the SX-V security systems; LightGard Generic Wireless, which allows you to use a 9 VDC wireless transmitter which is compatible with your current system; and LightGard Hardwired, which allows you to connect LightGard to your hardwired security system.

Note: The LightGard Wireless can also be used with the CareTaker® and RF Commander® systems if you put them on 24-hour protection and follow the programming instructions in your CareTaker or RF Commander manual. LightGard is best suited to the SX-V system, and this manual is written with that configuration in mind. The LightGard Wireless cannot be used with ITI LearnMode transmitters for the CareTaker *Plus*.

Note: The FCC notice on page iii applies only to the LightGard Wireless with SX-V transmitter. FCC compliance using non-ITI wireless products is the sole responsibility of the installing dealer.

1.1 Installation Summary

To install the LightGard system, follow these steps:

Table 1.1 Installation Summary

Step	Description	See
1	Select equipment to be protected and determine LTM location, cable route and maximum length.	Section 2
2	Install all necessary carrie nuts and cable trap accessories.	
3	Run the fiber-optic cable and install splices where needed.	
4	Make hardwired connection of LightGard to existing security system (hardwired LightGard only)	Section 3
5	Program the transmitter in the wireless Light-Gard	
6	Mount the LTM.	Section 3
7	Arm and test the system.	Section 4

1.2 Hints for the Installation Technician

This section contains ideas to make installation easier, faster, and more profitable.

- Always have the end user check the equipment to be protected to make sure it is operational before you install the system. After you have installed the system, have the end user check the equipment again.
- If you are installing the LightGard unit on an existing security system, locate the RJ31X at the site before you begin installation. If you are installing a new SX-V security system for the LightGard device, install the RJ31X within 5 feet of the system control panel.
- A tool that makes it easy to open up Macintosh® equipment is available through many Apple® Computer distributors or retail stores.
- When you are protecting large items with the LightGard, always open the equipment case. This helps you assess the best way to run the fiber-optic material through the inside boards and components, or if you can use carrie nuts.

Note: The operating temperature for the LightGard Unit is 40° to 100° F. For the fiber-optic loop, the operating temperature is 20° to 170° F.

Section 2 Installing Cable and Accessories

This section explains how to plan and install the LightGard fiber-optic cable and accessories, and how to secure specific pieces of equipment.

2.1 Using Fiber-Optic Cable

LightGard uses plastic fiber-optic cables rather than glass cables because plastic cable is easier to work with and much less expensive. The plastic fiber can be cut, spliced, and maintained more easily than can glass cable. The fiber-optic cable is available in rolls of 100 and 500 feet.

Using fiber-optic materials rather than electrical wire to provide a protection loop for specific pieces of equipment has four main advantages:

- Fiber optics are more difficult to defeat than electrical wire. Because the fiber-optic cable carries a timed-pulse light signal, it is impossible to shorten, bypass, or "jump" the fiber without causing a detectable interruption of the signal. An electrical circuit can be easily bypassed, since the circuit is always either open or closed.
- Fiber optics do not cause electromagnetic interference. Because the LTM sends a pulsed beam of light through the fiber-optic cable, you can loop the cable through and past sensitive electronic equipment without causing electromagnetic damage.
- It is easy to splice fiber-optic cables. This gives you maximum flexibility for changing or adding new equipment to your "protection loop."
- You can tie-wrap the cable with other existing wires. This provides strain relief from routine tugging and pulling which occurs as the machine is used.

Precautions When Using Fiber-Optic Cable

While fiber-optic cable offers distinct advantages over other equipment protection systems, you should still observe the following cautions:

- Be careful to run the loop so that it cannot be accidentally kicked or cut.
- If you use tie-wraps, do not tighten them so that they crush the fiber cable.
- Avoid sharp bends when running the fiber-optic cable. Sharp bends will attenuate (reduce) the pulsed signal. Wherever possible, keep bends to that they are never less than the cur-

vature of a quarter. Bends equal to the curvature of a dime will greatly attenuate the signal.

- Do not run the fiber-optic cable near sharp or rough edges that could nick or cut it.
- Do not run the cable near internal components that could become hot enough to melt the plastic. The operating temperature range for the fiber-optic cable is 20° to 170° F.

2.2 Maximum Cable Length for Splice Points

The maximum length of a single fiber-optic protective loop is limited and is decreased by the use of splices and sharp bends. You should determine the number of splice points you want to use carefully, because there is a trade-off between number of splices and maximum cable length. The more splices you use, the shorter the maximum cable length. The following chart shows the maximum recommended cable length for a given number of splices.

Table 2.1 How Splices Affect Maximum Cable Length

Number of Splice Points	Recommended Cable Length *
0	500 feet
1	400 feet
2	300 feet
3	250 feet
4	200 feet
5	150 feet

* Maximum cable length refers only to the length of the fiber-optic protection loop and does not affect the distance to the control panel.

Note: If you use carrie nut and cable trap fiber-routing accessories (described later in this chapter), you can cut down on the number of splices you need to use to complete your protection loop.

2.3 Splice Points and Accessories

A splice point is a pull-apart connection in the fiber-optic material which allows you to easily relocate or service equipment as necessary. You can use single and double splice points in combination on the same fiber-optic loop.

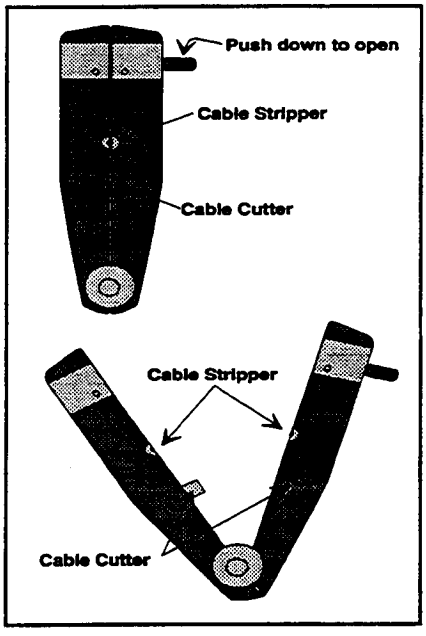

Figure 2.1 Cable Splicing Tool, Closed and Open

Single Splice Points

A single splice point consists of two male connectors joined by a double female connector. Single male connectors are available in packages of ten, and double female connectors are available in packages of five.

Splicing Plastic Fiber-Optic Cable

This section describes how to splice cable and how the various connectors work. To splice fiber-optic cable for the LightGard system, you will need the cable splicing tool shown in Figure 2.1.

1) Cut the fiber-optic material at the point at which you want to make a splice. Use a sharp razor blade or Exacto-knife.
2) Use the splicing tool to remove about 1/2 inch of the black jacket that protects the fiber core. Open the splicing tool and insert the cable into the cable stripper slot. Close the tool and twist, as shown in Figure 2.2.
3) Pull the cable away from the cutter, as shown in Figure 2.3.

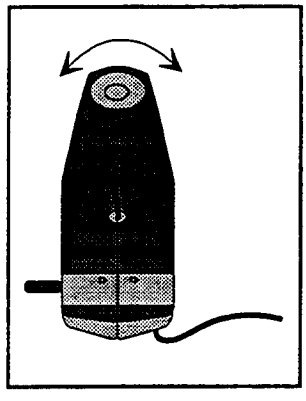

Figure 2.2 Fiber-Optic Cable Inserted in the Splicing Tool for stripping

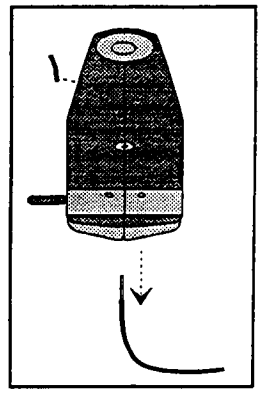

Figure 2.3 Stripping Fiber-Optic Cable

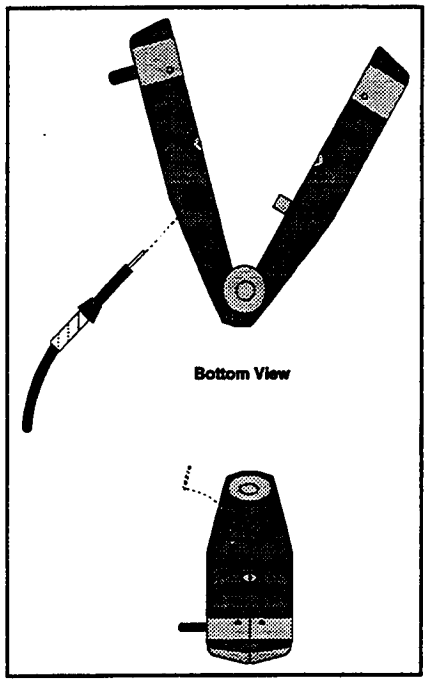

Figure 2.4 Completing a splice with the splicing tool

4) Check for core nicks by "flicking" the stripped end of the fiber with your finger. If the core was nicked, the stripped portion of the fiber will break off. If this happens, repeat steps 2 and 3.
5) Push the stripped end of the fiber material into the back of the male splice connector **as far as it will go**. The excess core material will extend through the front end of the male splice connector (see Figure 2.4).
6) Insert the male splice connector into the cable cutter hole on the back of the splicing tool, as shown in, so that the excess core material extends through the splicing tool.
7) Carefully squeeze the splicing tool until it is closed to cut off the excess fiber. When finished remove the cable from the stripping tool. The fiber-optic material will extend slightly beyond the end of the male connector.

8) You can now plug the male connector into any female connector.
9) To make a complete splice, repeat this procedure for the facing end of the fiber-optic cable. Plug two male connectors into the female connector to make a complete splice (see Figure 2.5).

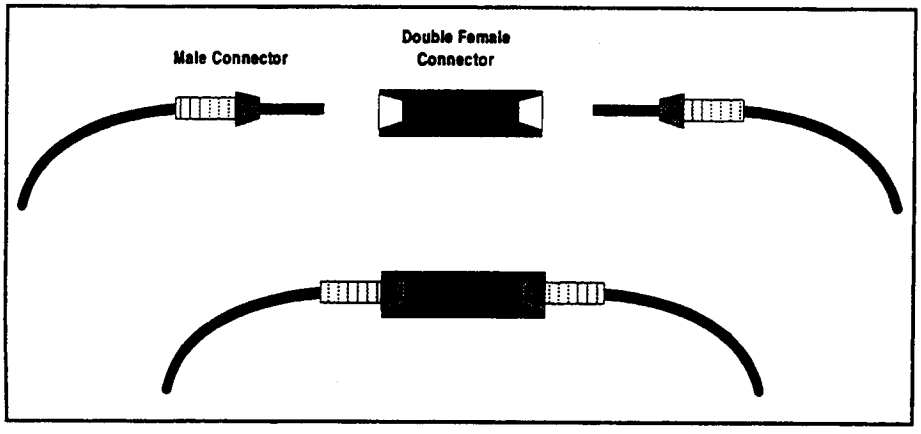

Figure 2.5 Connectors needed for a complete splice point

Note: Use splice optical couplant fluid to improve the contact point between the spliced ends of the fiber-optic cable. Put a little of the couplant compound on one of the male connectors before plugging it into the female connector. You only have to use it on one male connector in each splice.

Using Carrie Nuts

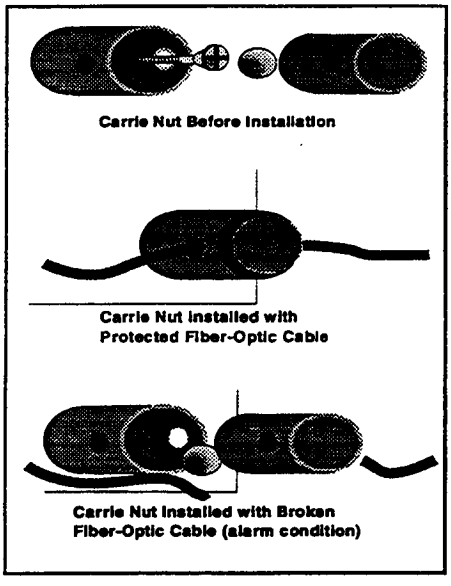

Figure 2.6 Using a Carrie Nut

Carrie nuts are fiber-routing devices which can be used to secure metal-framed equipment. They attach to the outside of the equipment that is being protected, and allow the fiber-optic cable to pass through it. Any attempt to remove the carrie nut sheath cuts the fiber-optic cable and results in an alarm condition. Figure 2.6 shows how the carrie nut works.

1) Identify a solid screw hole on the item to be protected. Be sure the screw can be threaded into metal.

Note: Do not use carrie nuts when a solid screw hole cannot be identified. Many current Apple Computers have plastic screws that do not thread into the chassis of the device.

2) In most cases, the screw provided with the equipment is not long enough to secure the carrie nut. we recommend using a 8x32 size screw when possible. To determine the maximum screw length you can use, open the case and check the distance between the hole you will be using to mount the carrie nut and the internal components. Close and secure the equipment case.

Note: Use a high-quality screw to secure the carrie nut. If you use a low-quality, soft, or brittle metal screw, it may be possible for the thief to knock the carrie nut off the protected component without breaking the fiber-optic loop.

3) Use the screw to secure the base of the carrie nut to the equipment to be protected. Tighten the screw so that the whole Carrie Nut Assembly will be able to turn freely without loosening the screw.

Note: We recommend that you use LockTite 242 Threadlock (or equivalent) on the threads of the screw.

4) Place the ball bearing in the base of the carrie nut and place the sheath over it. Align the holes in the base and sheath of the carrie nut.

   The ball bearing in the carrie nut prevents anyone from bending a screwdriver and inserting it through the hole, past the fiber and unscrewing the screw.

5) Pass the end of the fiber-optic cable through the carrie nut. Be sure the ball bearing is between the cable and the securing screw.

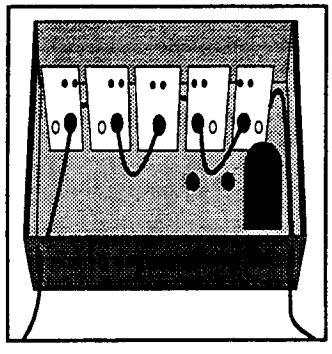

Figure 2.7 Direct Loop through Equipment and Internal Components

Using Direct Fiber-Optic Loops

For some pieces of equipment, it may be preferable to loop the fiber-optic cable directly through the equipment chassis and internal components. This is called a direct loop (see Figure 2.7).

A direct loop requires a 3/8-inch hole; this allows a splice point to pass through, and gives you greater flexibility when moving equipment or swapping cables. You can also use a 5/32-inch hole in the equipment, but this will only allow the cable to pass through (you must add the splice point after looping the cable through the equipment). We recommend that you use 3/8-inch holes whenever possible.

Do not run the fiber-optic line through vent holes or access ports, which could easily be cut out with little damage to the equipment. Loop the cable through as much of the equipment as possible to provide the greatest possible security.

Using Cable Traps

Cable traps are fiber-routing devices which deter theft by protecting the cables to which hardwired (nondetachable) peripheral devices such as mouses or keyboards are attached (see Figure 2.8). Cable traps come in four models to accommodate four common cable sizes.

Table 2.2 Size of Cable for Cable Traps

Cable Trap Name	Maximum Cable Size
Mouse Trap	3/16 inch
Rat Trap	1/4 inch
Squirrel Trap	1/2 inch
Cat Trap	5/8 inch

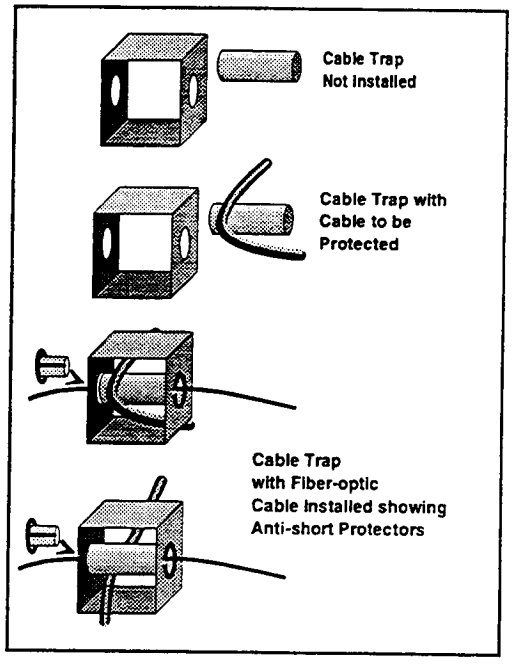

Figure 2.8 Protecting Peripheral Cable with a Cable Trap

Section 3 The LightGard Transceiver Module (LTM)

This section describes the LTM for each of the three configurations and how it is installed and mounted.

There are three basic LightGard configurations: the LightGard Wireless (SX-V), which is designed to work with the SX-V security system; the LightGard Generic Wireless, which can be used with most other 9 VDC wireless security systems; and the LightGard Hardwired, which can be used with most hardwired security systems.

All three LightGard configurations have a LTM which sends the alarm signal to the control panel. An alarm condition occurs when the fiber-optic loop is broken or the LTM itself is tampered with.

Note: The FCC notice on page iii of this manual applies only to the Wireless LightGard unit using an SX-V transmitter. It is not applicable to the Generic Wireless LightGard unit. Responsibility for determining FCC compliance using non-ITI wireless products is the sole responsibility of the installing dealer.

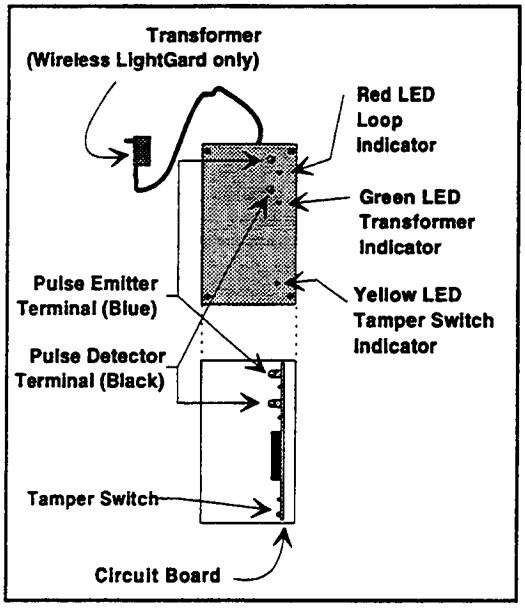

Figure 3.1 Internal and External Features of the LightGard

Every LTM contains a circuit board that consists of the tamper switches, the LED (light-emitting diode) service indicator lights, the pulsed beam emitter and detector, and the LightGard electronics that control the system (see Figure 3.1).

The tamper switch causes an alarm condition if the cover of the LTM is removed. On LightGard wireless units, an additional tamper switch is activated when the LTM is removed from its mounting surface.

There are three service indicator lights on the LTM. Table 3.1 illustrates what each LED indicates.

Table 3.1 Service Indicator Lights

Indicator Light	LED ON	LED OFF	LED Blinking
Red	Loop is bad. Alarm condition.	Loop is good.	Loop too long or bad splice
Green*	Transformer power is good.	Transformer power is bad.	N/A
Yellow	Tamper switches are bad or not depressed. Alarm condition.	Tamper switches are good.	N/A

* There is no green transformer indicator light on the hardwired LightGard unit.

Gel Cell battery will last for 3-5 years before you will have to replace it. You should replace it when it does not hold a charge.

When you restore the primary power source, the LightGard device automatically recharges the Gel Cell battery, a process that takes from 4-6 hours. LightGard unit is fully operational while the Gel Cell is recharging.

Advantages of the LightGard SX-V

Here are a number of advantages to using the LightGard device with the SX-V transmitter with the SX-V security system:

- The SX-V equipment has a special intrusion protection level (level 1 in the *SX-V System Installation Manual*). This allows you to designate and arm any of 61 transmitters to operate as a 24-hour sensor. In this way, transmitters installed as part of the LightGard system can be used to protect equipment on a 24-hour basis. This protection can be in force even if interior/exterior protection such as door/window and motion detectors are disarmed.
- When an alarm condition exists, each transmitter reports a unique number to the control panel and the central monitoring station. This provides fast, accurate dispatching in large facilities and third-party verification of alarm conditions.
- You can easily bypass a transmitter since each transmitter has its own unique number. This lets you perform maintenance on the equipment protected by one LTM without compromising or turning off the security on any of the other LightGard units.
- Every 69 minutes, each sensor sends a supervisory signal to the CPU. If the CPU does not "hear" any signals from a given transmitter for 12 hours, the "Supervisory" LED on the CPU lights and the transmitter number appears in the display.
- The SX-V can be set to a house code from 1 to 254. Use different house codes to prevent radio frequency (RF) interference between security systems that are close together.
- The handheld touchpad of the SX-V security system can be removed from the protected location to keep unauthorized people from tampering with it. The SX-V installation and owner's manuals have complete details on arming codes and security controls, which add greater versatility to the LightGard system.
- You can define an access code that disarms door and motion sensors but will keep the LTM armed.

Programming the SX-V Transmitter

To complete the programming of the LightGard, consult your *SX-V System Installation Manual*. The following procedures explain the process for programming and installing the LightGard Wireless SX-V unit (see Figure 3.3).

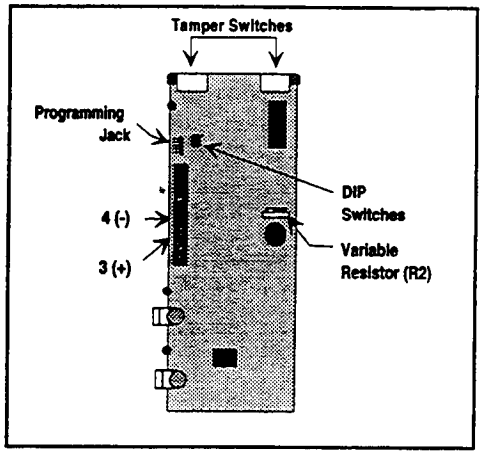

Figure 3.3 LightGard Wireless SX-V Circuit Board

Preparing the LTM for Programming

The following steps explain how to prepare the LTM and the SX-V door/window transmitter in the LTM for programming.

1) Plug the transformer into a 120 VAC outlet.
2) Open the LTM.
3) Disconnect the terminal wire from the positive battery terminal.
4) Attach a voltage meter to the terminal strip on the LightGard circuit board: positive lead to Terminal 3, negative lead to Terminal 4 (see Figure 3.3).
5) Adjust the variable resistor (R2) until the voltage reading is 6.8 V.
6) Reconnect the terminal wire to the positive battery terminal.

Programming the Door/Window sensor in the LTM

The following steps explain how to program the SX-V door/window sensor in the LTM. Before doing this procedure, you must complete the previous procedure, "Preparing the LTM for Programming."

1) Turn DIP switch 2 OFF. The center of the emitter terminal (blue) should be flashing red.
2) Depress both tamper switches and keep them depressed through steps 3 through 8.
3) Attach the SX-V programmer to the program jack on the LightGard circuit board (see Figure 3.3).

Note: Be sure you attach the programming plug so that the open side of the plug faces the top of the circuit board.

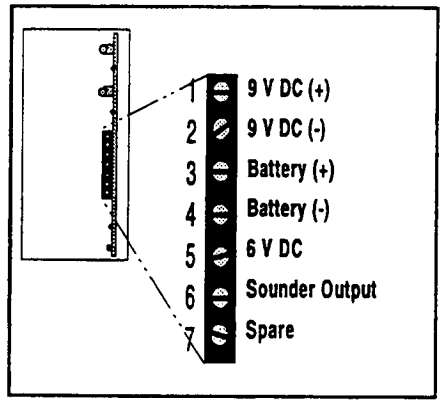

Figure 3.4 LightGard Wireless SX-V Wiring Diagram

4) Set the transmitter house code as indicated in the *SX-V System Installation Manual.*
5) Set the transmitter sensor number as indicated in the *SX-V System Installation Manual.*
6) Set the transmitter sensor type to "0" (Freeze Sensor). This tells the transmitter to send "restore reports" when the fiber-optic loop is reconnected or restored.

Note: It is very important that you program the sensor to report a restore condition. This initiates a "refusal to arm" signal if a fiber-optic loop is not properly closed, and prevents the system from arming that sensor until the problem is corrected. It will also tell the central monitoring station which sensors are bypassed during an alarm condition.

7) Disconnect the programmer from the LightGard program jack.
8) Turn DIP switch 2 ON.

Completing the Programming Process

The following steps explain how to program the SX-V door/window sensor in the LTM. Before doing this procedure, you must complete the previous procedures, "Preparing the LTM for Programming" and "Programming the door/window sensor in the LTM."

1) Mount the LTM according to the mounting instructions in section 3.5.
2) Initialize the unit by closing and opening the loop as described in section 3.5.
3) After you have installed all the sensors, program the LightGard sensors into the CPU as indicated in the *SX-V System Installation Manual*, and contact the Central Monitoring Station.
4) Have the Central Monitoring Station set the Control Panel to use group command number "03" and letter code "L" for the LightGard units. This makes all the LightGard transmitters active at level 1, and causes the SX-V to report "Low Battery" when such a condition exists.
5) Use the F10 (Signal Strength Indicator) feature when installing your sensors. This helps ensure that the sensors are within transmitting range of the CPU and reduces the number of supervisory reports from the system. For more information, see your *SX-V System Installation Manual.*

   We recommend that you program your SX-V CPU with the option numbers in Table 3.2.

Table 3.2 SX-V Options Recommended When Using the LightGard Device

Option	Description
00	Alarm! Buddy System!
77	Touchpad Tamper
84	Opening Report User N
85	Closing Report User N
87	Auto Force Armed
90	AC Power Failure
92	Alarm! Tamper Loop
93	Automatic Phone Test

We also recommend that you use the optional features in Table 3.3.

Table 3.3 SX-V Optional Features Recommended When Using the LightGard Device

Optional Feature	Description
F04	Low Battery Report
F07	Open Sensor Display
F14	Hourly Phone Test
F15	Sensor Tamper

For more information on these options and optional features, consult the *SX-V System Installation Manual.*

Note: Before arming the system, close, open, and reclose the fiber-optic loop.

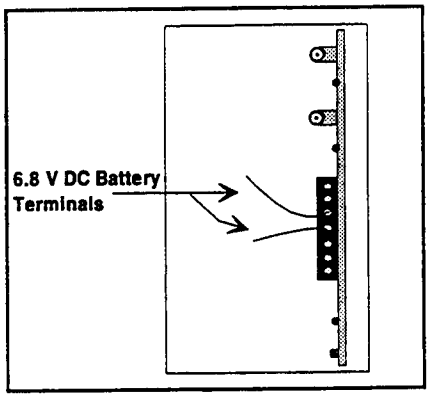

Figure 3.5 LightGard Generic Wireless Diagram

3.2 Wireless LightGard (Generic)

The generic wireless LTM does not include a transmitter. It interfaces with most 9 V wireless transmitters which are no larger than 3/4" x 1-3/4" x 3-1/8". Program the wireless transmitter according to the instructions in the equipment installation manual. Be sure to program the transmitter and CPU so that the LightGard is armed as a 24-hour device.

Note: The FCC notice on page iii of this manual applies only to the Wireless LightGard unit using an SX-V transmitter. It is not applicable to the Generic Wireless LightGard unit. Responsibility for determining FCC compliance using non-ITI wireless products is the sole responsibility of the installing dealer.

After you have programmed your transmitter, wire the transmitter to the LightGard circuit board. Refer to Figure 3.5, Figure 3.6, and the following instructions.

1) If the transmitter is normally open, connect the transmitter to Terminal 9 (common) and Terminal 10 (normally open).

or– If the transmitter is normally closed, connect the transmitter to Terminal 8 (normally closed) and Terminal 9 (common).

2) Connect Terminal 5 (9 V positive) to the positive input on your transmitter.

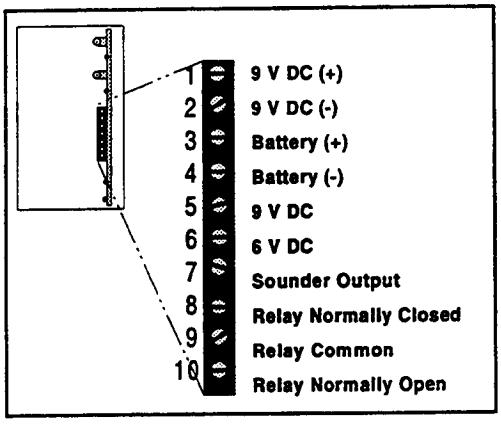

Figure 3.6 LightGard Generic Wireless Wiring Diagram

Warning: Do not use the battery that comes with your transmitter. Power your transmitter from the LightGard power supply. If your transmitter requires that you use the batteries supplied by the manufacturer, please contact ITI Technical Services.

3) Connect Terminal 4 (negative) to the negative input on your transmitter.

4) Mount the LTM according to the mounting instructions in section 3.5.

Note: Before arming the system, initialize the unit by closing and opening the loop as described later in this section.

3.3 LightGard with Keyswitch and Sounder

Note: The wiring and programming method for the LightGard with keyswitch and sounder is identical to the programming method for other Generic or SX-V Wireless units.

The keyswitch mechanism turns the sounder on and off. The setting of the key switch determines if the sounder will be activated in case of an alarm.

If the keyswitch is in the ON position and an alarm condition occurs, the alarm signal will be sent to the control panel and the sounder is activated. The sounder will continue to sound until the key is turned OFF.

If the keyswitch is in the OFF position and an alarm condition occurs, the alarm signal is sent to the CPU, but the sounder remains silent (see Figure 3.7).

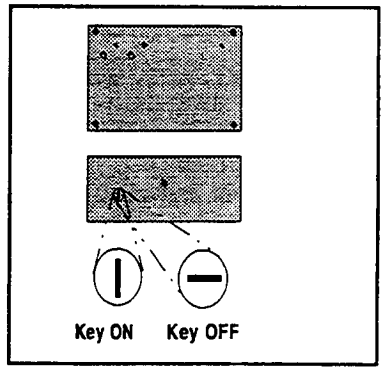

Figure 3.7 LTM with Keyswitch for Sounder

3.4 Hardwired LightGard

The hardwired LightGard uses 12 VDC power supplied by the alarm control panel. This section describes supervised and unsupervised circuits, and a wiring diagram (see Figure 3.9).

Warning:
Always use the LightGard device with an alarm control panel that has an adequate power supply to provide 500 mA at 9 VDC for each LightGard unit. In some cases, you need to add a supplemental power supply. You also need an adequate backup power supply for the control panel to ensure that the device operates properly in the case of a temporary power outage.

Supervised Hardwired LightGard

In supervised mode, as soon as you apply power to the hardwired LightGard device, an internal relay becomes energized. If the wire that supplies power is disconnected or if an alarm condition exists, the relay de-energizes and the panel activates an alarm.

To select supervised mode, open the LTM and locate the slide switch on the circuit board. Move the slide switch to the left, as illustrated in Figure 3.8. In supervised mode, the LightGard device draws 70 mA in standby and 35 mA in alarm.

Note: There is no end-of-line resistor matrix provided with the hardwire LightGard device. This lets you use whatever end-of-line resistor is recommended with your alarm control panel.

Unsupervised Hardwired LightGard

In unsupervised mode, the internal relay becomes energized when an alarm condition exists. This causes the panel to activate an alarm.

To select unsupervised mode, open the LTM and locate the slide switch on the circuit board. Move the slide switch to the right, as illustrated in Figure 3.8. In unsupervised mode, the LightGard device draws 35 mA in standby and 70 mA in alarm.

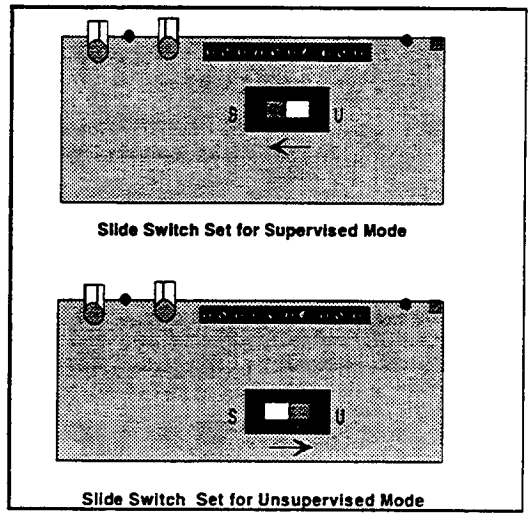

Figure 3.8 Slide Switch on Hardwired LightGard Circuit Board

Mount the LTM according to the mounting instructions in section 3.5.

Note: Before arming the system, initialize the unit by closing and opening the loop as described in section 3.5.

Note: See Figure 3.9 for wiring diagram for the Hardwired Lightgard which shows the terminals you need for supervised and unsupervised use.

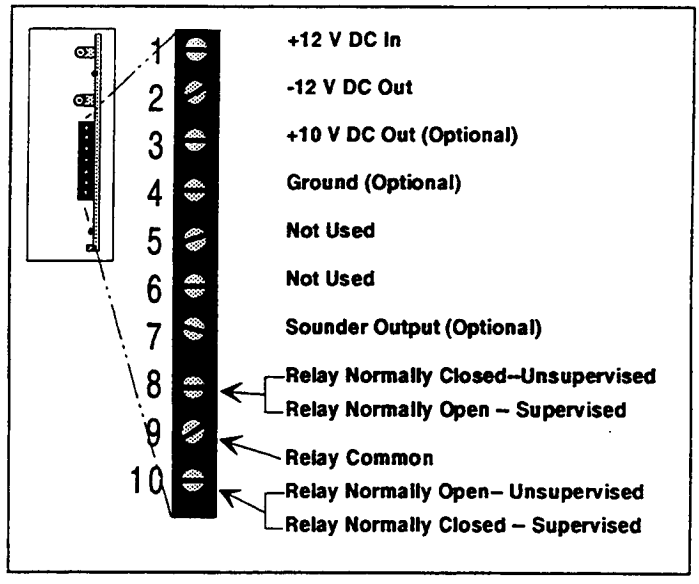

Figure 3.9 Hardwired LightGard Wiring Diagram

3.5 Mounting the LTM

This section describes the process of mounting the wireless and hardwired LTMs.

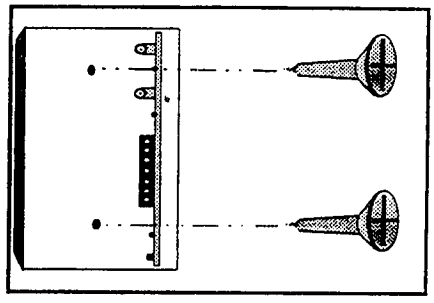

Figure 3.10 Mounting the LTM

Wireless LightGard

Note: Place the unit where it will not be kicked or bumped. This prevents damage to the equipment or alarms from the tamper switches or from accidentally disconnecting the fiber-optic cable.

The wireless LightGard can be mounted in either of two ways:

- Open the LTM. Use panhead or flathead screws through the two screw holes in the bottom of the box to attach the box to the table, desk, or wall (see Figure 3.10).
- Use the two angle brackets included in the mounting kit to mount the LTM under the desk or table. Use the 6 x 3/8" self-tapping screw to attach the bracket to the box, and the 6 x 3/4" self-tapping screw to mount the bracket to the table or desk (see Figure 3.11).

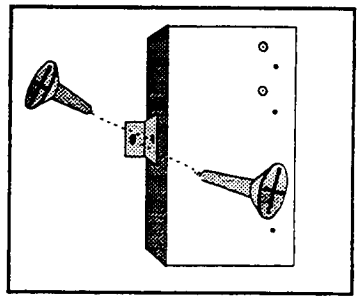

Figure 3.11 Using Brackets to Mount the LTM

Hardwired LightGard

To mount the hardwire LightGard LTM, open the LTM and drill two holes in the back of the box. Use panhead or flathead screws through these holes to attach the box to the table, desk, or wall (see Figure 3.10).

Note: The hardwired LightGard has no tamper device on the back of the LTM because the device is wired to the control panel. Any tampering will break the circuit and cause an alarm condition.

Section 4 Testing and Servicing

This section includes instructions for testing the LightGard device. Test procedures for the LightGard device on generic wireless systems (other than the SX-V) or hardwired systems vary from manufacturer to manufacturer. Please consult the installation or owner's manual for information on testing and arming a door/window sensor.

This section also contains a troubleshooting table with solutions to circumstances that may occur during installation.

4.1 Testing the LightGard Device

This procedure describes general testing steps.

Note: Before arming the system, initialize each Light Transceiver by closing, opening, and reclosing the loop.

1) Arm the system for a sensor test (level 9 on the SX-V).
2) Open the protection loop of each LTM and cause an alarm condition. At the CPU, verify that each LTM is working correctly.
3) Close each protection loop.
4) **If you have a LightGard wireless device,** open the lid of the Light Transceiver and be sure the tamper switch trips the system. Replace the lid on the LTM.

or– **If you have a LightGard hardwired device,** disconnect the supervised wire that runs between the LTM and the control panel and be sure the system detects the alarm condition. Reconnect the LTM and the control panel.

5) Reset the system by opening and closing the fiber-optic loop.

4.2 Troubleshooting

Table 4.1 describes various situations, causes, and solutions.

Table 4.1 Causes and Solutions when Troubleshooting

Indication	Cause	Solution
Red Service Indicator Light Lit	Detector is not receiving signal sent by emitter.	The protection loop is too long, or there are too many splices for the length of the loop.
		Splice point is defective or poorly made.
		Fiber-optic cable is improperly inserted into the screw terminals.
		Cut, nick, or break in fiber-optic material. See section 4.3 "Tracing a Break in Fiber-Optic Cable."
System Will Not Arm	LTM is in alarm condition.	Protection loop is broken, unit has been tampered with. If unit is hardwired, check wiring between LTM and CPU.
		Check internal wiring in the LTM.
Transceiver reports Low Battery condition.		Check to be sure that the 9 VDC power supply is plugged into 120 VAC power. Plug transformer in, and the batteries will recharge.
Supervisory	The transformer is unplugged and the battery is not strong enough to allow transmitter to report in.	Check to be sure that the 9 VDC power supply is plugged in to 120 VAC power. Plug transformer in, and the batteries will recharge.
	Transmitter is out of range.	Relocate transmitter or CPU.
	Transmitter is not working properly.	(SX-V) Program control panel in F-10 mode and trip any transmitter showing this problem. The control panel will tell you the strength of your transmitted signal. See section 4.4 "Testing Transmitter Range without a Control Panel."
		Call ITI Technical Services, 1-800-777-2624
		Consult manufacturers installation manual for all other types of equipment.

4.3 Tracing a Break in Fiber-Optic Cable

1) Remove both ends of the fiber-optic loop from the terminals on the LTM. Look at the emitter, and you will see an intense, pulsing red light.
2) If you do not see the light, be sure the Transceiver is connected to the power supply (9 VDC transformer, or hardwire to CPU).
3) Replace one end of the fiber-optic loop in the emitter (blue) terminal. Look at the other end of the cable and see if you see the light at that end.
4) If you see the intense red light, the fiber-optic loop is **intact.** If the light is dim or pulses irregularly, go to the next step.
5) Remove the next length of fiber-optic cable up to the next splice point. Look at the end of the cable and see if the light is visible at that end.
6) Repeat the previous step until the light is intense and clearly visible at the end of the fiber-optic cable.
7) The piece of cable that you remove just before the light becomes clearly visible is the faulty length of cable.
8) Remake that piece of cable using new male splice connectors and cable. Discard the old cable and complete the fiber-optic loop.

4.4 Testing Transmitter without a Control Panel

If you are not able to use an active control panel to test a transmitter and you are working with a wireless LightGard device on the workbench, use the following procedure to test the quality of your transmitters' radio frequency (RF) signals.

Test Method One

Use the RF Sniffer to determine the quality of the transmitted signal.

Test Method Two

You need:

Radio Shack 277-1008 Audio Amplifier

Model IN 914 Diode

1/8" phono jack

Two-conductor wire

1) Attach the diode across the conductors at one end the wire.
2) Attach the phono jack across the conductors at the other end of the wire.
3) Plug the phono jack into the input jack of the audio amplifier.
4) Turn on the audio amplifier and set volume as desired.
5) Hold the diode end of the wire close to the transmitter and activate the transmitter.

   You will hear the data burst as an audible signal each time the transmitter is activated.

Appendix A Product List

The following Product List includes the LightGard products and accessories, as well as installation manuals referred to in the *LightGard Device Installation Manual.*

Note: ITI reserves the right to make changes to this product list without notice.

Part #	Description.
60-550	LightGard Wireless with SX-V Transmitter
60-549	LightGard Wireless with SX-V Transmitter, Key and Sounder
60-539	LightGard Generic Wireless
60-538	LightGard Generic Wireless with Key and Sounder
60-537	LightGard Hardwired
60-536	LightGard Hardwired with Key and Sounder
60-535	Carrie Nut Assembly
60-531	Mouse Trap Assembly
60-532	Rat Trap Assembly
60-533	Squirrel Trap Assembly
60-534	Cat Trap Assembly
13-328	Cable Splicing Tool
60-544	Single Male Splice Connectors (pack of 10)
60-542	Double Female Splice Connectors (pack of 5)
60-540	Splice Point Set – 10 pack (20 male and 10 female)
60-547	Fiber-optic cable, 500 foot spool
60-548	Fiber-optic cable, 100 foot spool
13-312	Splice Optical Couplant
40-315	$5\,^{1}/_{2}$" Tie Wraps
46-599 B	*LightGard Installation Manual*
46-074	*SX-V Installation Manual*
46-065	*CareTaker Installation Manual*
46-284	*RF Commander Installation Manual*

Glossary

alarm condition
any situation that would cause an alarm signal to the CPU. On the LightGard device, alarm conditions are caused by any break in the fiber-optic loop or tampering with the LTM.

cable trap
a device that deters theft by securing the cables of hardwired equipment. A fiber-optic loop runs through the cable trap, and any attempt to remove the protected cable will sever the fiber-optic material, causing an alarm condition.

carrie nut
a device that secures metal-framed equipment. When the carrie nut is secured to the equipment, a fiber-optic loop runs through the carrie nut. Any attempt to remove the equipment or carrie nut sheath severs the fiber-optic material, causing an alarm condition.

detector
receives and analyzes the pulsed light signal sent through the fiber-optic cable. The detector terminal is the black terminal on the cover of the transceiver.

direct loop
A direct loop is used when a carrie nut or cable trap cannot be used to secure a piece of equipment. To create a direct loop, run the fiber-optic cable directly through the equipment and internal components to be protected.

emitter
sends the pulsed light signal through the fiber-optic cable. The emitter terminal is the blue terminal on the cover of the transceiver.

fiber-optic
a method of sending light or light pulses through the transparent core of a cable-like material. Fiber optics are often used for point-to-point communication.

fiber-optic cable
an insulated cord that contains one or more fiber-optic lines. The fiber-optic cable used in the LightGard device has a single-line core.

gel cell battery
a backup power source for the SX-V LightGard device. It provides 6 VDC and is recharged as needed by the primary LightGard power supply.

hardwired
any security system that has its sensors connected to the control panel by wired connections is said to be hardwired.

internal theft
any loss that is directly attributable to employees, students, staff, and other personnel who have access to equipment.

light transceiver module (LTM)
is the main unit for the LightGard device. It contains the terminals for the fiber-optic loop and the light emitter and detector circuitry, as well as the tamper switch. In wireless LightGard units, the transceiver also holds the transmitter.

LTM
See light transceiver module.

splice
the way of connecting the ends of two pieces of fiber-optic cable to make an optical connection between them.

supervised sensor
a sensor that sends a signal to the CPU on a regular basis. This signal tells the CPU that the sensor is operating correctly and helps prevent problems before an alarm condition arises.

tamper switch
a momentary switch attached to the LTM. It triggers an alarm condition if the cover of the LTM is removed, or (in the case of the wireless LightGard devices) if the unit is removed from its mounting surface.

unsupervised sensor
a sensor that sends only alarm signals to the control panel. The control panel, then, has no way of monitoring the "health" of the sensor. Since there is no way to automatically assess the operation of the sensor, without regular sensor checks, it is more likely that the sensor will be inoperative when an alarm condition arises.

wireless
any security system which has its sensors connected to the control panel by RF transmitted signals is said to be wireless.