T-Link TL250

Network Internet Alarm Communicator

Installation Manual

version 1.0

WARNING Please Read Carefully

Note to Installers

This warning contains vital information. As the only individual in contact with system users, it is your responsibility to bring each item in this warning to the attention of the users of this system.

System Failures

This system has been carefully designed to be as effective as possible. There are circumstances, however, involving fire, burglary, or other types of emergencies where it may not provide protection. Any alarm system of any type may be compromised deliberately or may fail to operate as expected for a variety of reasons. Some but not all of these reasons may be:

Inadequate Installation

A security system must be installed properly in order to provide adequate protection. Every installation should be evaluated by a security professional to ensure that all access points and areas are covered. Locks and latches on windows and doors must be secure and operate as intended. Windows, doors, walls, ceilings and other building materials must be of sufficient strength and construction to provide the level of protection expected. A reevaluation must be done during and after any construction activity. An evaluation by the fire and/or police department is highly recommended if this service is available.

Criminal Knowledge

This system contains security features which were known to be effective at the time of manufacture. It is possible for persons with criminal intent to develop techniques which reduce the effectiveness of these features. It is important that a security system be reviewed periodically to ensure that its features remain effective and that it be updated or replaced if it is found that it does not provide the protection expected.

Access by Intruders

Intruders may enter through an unprotected access point, circumvent a sensing device, evade detection by moving through an area of insufficient coverage, disconnect a warning device, or interfere with or prevent the proper operation of the system.

Power Failure

Control units, intrusion detectors, smoke detectors and many other security devices require an adequate power supply for proper operation. If a device operates from batteries, it is possible for the batteries to fail. Even if the batteries have not failed, they must be charged, in good condition and installed correctly. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage electronic equipment such as a security system. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.

Failure of Replaceable Batteries

This system's wireless transmitters have been designed to provide several years of battery life under normal conditions. The expected battery life is a function of the device environment, usage and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. While each transmitting device has a low battery monitor which identifies when the batteries need to be replaced, this monitor may fail to operate as expected. Regular testing and maintenance will keep the system in good operating condition.

Compromise of Radio Frequency (Wireless) Devices

Signals may not reach the receiver under all circumstances which could include metal objects placed on or near the radio path or deliberate jamming or other inadvertent radio signal interference.

System Users

A user may not be able to operate a panic or emergency switch possibly due to permanent or temporary physical disability, inability to reach the device in time, or unfamiliarity with the correct operation. It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm.

Smoke Detectors

Smoke detectors that are a part of this system may not properly alert occupants of a fire for a number of reasons, some of which follow. The smoke detectors may have been improperly installed or positioned. Smoke may not be able to reach the smoke detectors, such as when the fire is in a chimney, walls or roofs, or on the other side of closed doors. Smoke detectors may not detect smoke from fires on another level of the residence or building.

Every fire is different in the amount of smoke produced and the rate of burning. Smoke detectors cannot sense all types of fires equally well. Smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches or arson.

Even if the smoke detector operates as intended, there may be circumstances when there is insufficient warning to allow all occupants to escape in time to avoid injury or death.

Motion Detectors

Motion detectors can only detect motion within the designated areas as shown in their respective installation instructions. They cannot discriminate between intruders and intended occupants. Motion detectors do not provide volumetric area protection. They have multiple beams of detection and motion can only be detected in unobstructed areas covered by these beams. They cannot detect motion which occurs behind walls, ceilings, floor, closed doors, glass partitions, glass doors or windows. Any type of tampering whether intentional or unintentional such as masking, painting, or spraying of any material on the lenses, mirrors, windows or any other part of the detection system will impair its proper operation.

Passive infrared motion detectors operate by sensing changes in temperature. However their effectiveness can be reduced when the ambient temperature rises near or above body temperature or if there are intentional or unintentional sources of heat in or near the detection area. Some of these heat sources could be heaters, radiators, stoves, barbeques, fireplaces, sunlight, steam vents, lighting and so on.

Warning Devices

Warning devices such as sirens, bells, horns, or strobes may not warn people or waken someone sleeping if there is an intervening wall or door. If warning devices are located on a different level of the residence or premise, then it is less likely that the occupants will be alerted or awakened. Audible warning devices may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners or other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a hearing-impaired person.

Telephone Lines

If telephone lines are used to transmit alarms, they may be out of service or busy for certain periods of time. Also an intruder may cut the telephone line or defeat its operation by more sophisticated means which may be difficult to detect.

Insufficient Time

There may be circumstances when the system will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time to protect the occupants or their belongings.

Component Failure

Although every effort has been made to make this system as reliable as possible, the system may fail to function as intended due to the failure of a component.

Inadequate Testing

Most problems that would prevent an alarm system from operating as intended can be found by regular testing and maintenance. The complete system should be tested weekly and immediately after a break-in, an attempted break-in, a fire, a storm, an earthquake, an accident, or any kind of construction activity inside or outside the premises. The testing should include all sensing devices, keypads, consoles, alarm indicating devices and any other operational devices that are part of the system.

Security and Insurance

Regardless of its capabilities, an alarm system is not a substitute for property or life insurance. An alarm system also is not a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergencysituation.

Table of Contents

Introduction Section 1

The T-Link TL250 is a network internet communicator that sends alarm system information to the central station.

The T-Link TL250 has four modes of operation. It can operate in one of three stand-alone operational modes or can be connected to a compatible DSC panel.

The T-Link TL250 is pre-programmed with the most commonly used settings for quick installation. Default options can be custom programmed using T-Link Console software if required.

Mode 1: Bell Follower

In Mode 1, the T-Link TL250 monitors the Bell Output of the control panel. The system identifies the Bell Output cadence and transmits the corresponding Fire or Burglar alarm reporting code to the central station.

Refer to the appropriate control panel *Installation Manual*.

NOTE: Do not use Mode 1 for UL Listed Installations.

Mode 2: 4-Zone Panel

In Mode 2, the system is configured for 4-zone, stand alone operation. Refer to Diagram B3 for more details.

Mode 3: 12-Zone Panel

If the T-Link TL250 detects a PC5108 expander card on power up it will automatically configure itself for 12-zone standalone operation with normally open loops. Refer to Diagram B4 for more details.

NOTE: In modes 2 & 3, the connections between the PC5108 inputs or T-Link TL250 inputs and the alarm control unit outputs (relay contacts) shall be done in metal conduit, within 20 ft. Stand-alone operation will still require the inputs to be programmed with the desired alarm types.

Mode 4: Standard Mode: In standard mode, the system is configured as a communicator with a compatible DSC alarm panel: Models PC4020, PC4020CF, PC5020 or PC5020CF.

2.1 Installation

1. Determine the Operating Mode Required

The operating mode (Modes 1, 2, 3 or Standard Mode) will determine how the unit is to be wired.

2. Determine the Mounting Location

Select a mounting location in a dry, protected area. The mounting location should be at least 30 cm. away from physical contact with

any person. See page 30, Appendix E, for Network Protection details.

NOTE: Do not exceed the following recommendations for wire run distances

- Input wiring should must be minimum 22 gauge quad (0.5mm). Two pair twisted is preferred.
- PC5108, or zone wiring must not exceed 1,000' (305m) (in wire length) from the T-Link TL250.
- Shielded wire is not necessary unless wires are run in an area that may present excessive RF noise or interference.
- Refer to section 5, Programming Descriptions, section [36] for zone wiring details.

3. Route Wiring to Mounting Location

Route wiring from the hardwired zones or control panel as required.

NOTE: Route wiring through conduit to a junction box if possible. Mount the T-Link TL250 Panel.

2.2 Testing

Standard Mode: Make sure the panel is programmed to use the T-Link TL250 in accordance with the settings outlined in Sections 4, Programming Guide . Simulate Burglar and Fire Zone violation on the DSC alarm panel. Verify that the T-Link TL250 transmits the events to the central station.

Mode 1: Make sure the T-Link TL250 Input 1 is programmed in accordance with the settings outlined in Sections 6, Programming Descriptions . Simulate Burglar and Fire Zone violation on the alarm panel. Verify that the T-Link TL250 transmits the events to the central station.

Mode 2 & 3: Simulate Inputs violations in accordance with the settings outlined in Sections 6, Programming Descriptions. Verify that the T-Link TL250 transmits the events to the central station.

2.3 Resetting to Factory Defaults

Standard Mode

- Enter section 999 of the T-Link TL250
- Enter 00 to default the unit to factory settings
- Enter 55 to restart the unit.

Mode 1, 2 and 3:

- Remove Power from the T-Link TL250; disconnect battery and control panel if applicable
- Disconnect all wiring from the PGM1 and IN1 terminals. Connect a jumper wire between the PGM1 and IN1 terminals
- Apply power to the system
- Remove power from the system
- Reconnect all original wiring and reapply power to the system
- Test System - refer to Section 2.2

NOTE: A restart is required for the programming changes to take effect. Allow up to 15 seconds for a restart.

The maximum allowable current draw from a compatible DSC panel on the Aux terminal Output is 500 mA @ 12VDC. Operational current draw of the T-Link TL250 is 250 mA. The T-Link TL250 module has 2 switched negative programmable outputs (50 mA @ 12 VDC).

- Input Voltage: 12 VDC
- Current: 250 mA (275 mA with PGM or PC5108)
- Dimensions: 3.25” × 5.25” (8.3 cm × 13.3 cm)
- Operating Temperature: 32°-122°F (0°-49°C)
- Output Protocols: UDP/IP 10/100 BaseT half duplex
- Input Protocols: PC-Link (SIA format)
- Connectors: 4-pin header for the PC-Link and RJ-45 for Ethernet
- Network: Ethernet LAN/WAN 10 BaseT or 10/100 BaseT
- Call Direction Options: primary or backup communicator using panel call direction
- Downloading Support for DSC Control Panel: DLS-3 and/or System Administrator software
- Programming: panel keypad, console on the RS232 or T-Link console remotely
- Multiple Central Stations: primary and backup via phone line*
- Approval Listings: FCC, IC, CE, UL (Grade of Service AA), ULC (Signal Channel Security Level 4/5)
- 4 digital inputs (can be increased to 12 using the PC5108)
- Capable of sending alarm messages to 2 e-mail addresses

NOTE: For UL Listed fire installations, shared on-premises communication equipment is required to be UL Listed for Information Technology Equipment. The communication medium between protected property and communications service provider must be for the exclusive use of the protected property and not shared with other communications service provider subscriber.

When a hub or router/gateway is used on the premises in conjunction with the T-Link TL250, 24-hr standby power is required for these devices (i.e., UL Listed UPS, battery backup).

The PGM2 output is used as an Input Follower where it will be triggered on any Input alarm (including the Bell Follower that generates Burglary and Fire Alarms) with the exceptions of a Keyswitch zone. The PGM2 output will only turn off when ALL violated zones are restored.

NOTE: This PGM is always enabled and following zones. It is the user’s decision to connect a device to the PGM.

CAUTION: The ethernet communication lines must be connected first to an Approved (acceptable to the local authorities) type NID (Network Interface Device) before leaving the premises (e.g., UL installations, UL60950 Listed NID).

4.1 Connecting the T-Link TL250 to the Power864 (PC5020) or Maxsys (PC4020) Panels

The power should be removed from the control panel before any connections are made to the T-Link TL250. Connect the 12VDC and GND terminals to the panel auxiliary power output. Connect the supplied cable from the T-Link TL250 white connector to the PC-Link header of the control panel.

The black wire of the PC-Link cable is pin 1 on the PC-Link header for the PC5020 v3.2 or higher control panels. The PC-Link header is polarized on the PC4020 v3.31 or higher control panel. Connect the e-ground to a proper earth-ground connection.

4.1.1 Stand-alone Setup

Connect the 12VDC and GND terminals to the external 12V power source.

NOTE: For UL Listed installations, a UL Listed power supply must be used.

4.2 Remote Control

The panel and the DLS software will control this function. The module will be a conduit for the information. Commands can be sent from the DLS or SA software to allow control of the panel; Arm/Disarm, Bypass/Un-Bypass, Status Request.

NOTE: New DLS-3 and System Administrator drivers are required for the PC5020 v3.2 and PC4020 v3.31. These drivers can be downloaded free from dsc.com/dls3drivers.htm. DLS-3 and System Administrator can communicate directly to the T-Link TL250 module. The DLS software can be used with UL Listed installations only when a service personnel are on-site.

4.3 Programming

The T-Link TL250 can be programmed remotely or locally with the T-Link Console Software via the ethernet connection or locally with the T-Link console via the serial port. Programming can also be done through the control panel when connected to a PC4020 or PC5020. TL250 programming cannot be done using DLS software.

NOTE: On a default unit the T-Link can be reached from the console at IP 192.168.0.99 with a subnet mask of 255.255.255.0 on port 3064.

4.4 Unique IP Address

Each T-Link on the same network node must have a unique IP address. This system is compatible with any device that masks the IP address of the originating device. DHCP can be used with the TL250.

For remote programming, the IP must be known by the T-Link console or the DLS/SA computer(s). For this reason, DSC recommends a Static IP or setting up the DHCP server to always license the same IP to the T-Link based on its MAC address.

4.5 Mounting the Module

For PC4020(CF)/PC5020(CF) control panel installations, refer to the PC4020(CF) and PC5020(CF) Installation Manuals respectively. Mount the T-Link on the side wall of the PC4050C or PC4050CR cabinet. Refer to page 30, Appendix E for Network Protection Installation Instructions. When used as a stand-alone configuration or in conjunction with the PC5108 module, install the TL250 in a DSC enclosure, model PC5003C.

4.6 Status Indicators

There are 4 LEDs on the board to indicate connection, traffic and trouble conditions.

LK LED (Link Status) will turn on when the network is present and will blink when there is network activity.

ACT LED (Activity/Network Traffic Status) will blink to show network activity.

SPD LED (Speed Status) will remain off for 10BaseT network connection and will be on to indicate 100BaseT network connection.

STAT (Status) LED will normally blink once every 5 seconds. If a trouble is present, the LED will blink a number of times (as per table) with a one second pause before restarting the sequence. If there is more then one trouble present, the LED will blink at a rate that is equal to the highest priority.

The transmitter has a number of individually maskable trouble conditions that report various troubles present on the transmitter. For the corresponding trouble toggle option, refer to section [033] and [034]. Options [033] and [034] can be set to ignore for any or all trouble conditions. Once a trouble is ignored, it will no longer generate a signal or have any affect on the Status LED.

Example: The network is not present and inputs are in alarm. The LED will blink once with a one-second pause. When the network trouble is cleared the LED will blink five times with a one-second pause.

Status	Number of Blinks/Priority	Description
Network Absent	1	The Ethernet link between the transmitter and local hub or router is absent. This is equivalent to the link LED on the Ethernet chip being off.
Invalid Account	2	The transmitter account code is still set to the default value of FFFFFF.
Receiver 1 Absent	3	The transmitter is not receiving Receiver Heartbeat commands from the receiver.
Panel Absent	4	The transmitter is not receiving polls from the DSC 4020 or 5020 panel through the PC-Link interface. Generic panels are not supervised by the transmitter.
Input Alarms	5	There are inputs on the T-Link which are in the alarm condition
FTC 1	6	T-Link failed to communicate with Receiver#1
PC5108 Absent	7	The PC5108 Module is not responding to the transmitter.
PC5108 Tamper	8	The PC5108 Module Tamper has been activated
FTC 2	9	T-Link failed to communicate with Receiver#2
Keyswitch Arm	10	The system was armed by the keyswitch zone
T-Link Remote Programming	11	T-Link is being programmed remotely
T-Link Local Programming	12	T-Link is being programmed locally
Receiver #2 Absent	13	The transmitter is not able to connect to Receiver#2 on power-up

Programming Guide Section 5

Before programming the T-Link TL250 module, obtain the following items from the Network Administrator:

1. The static IP address for the T-Link TL250 module (Section [001]).
2. The subnet mask for the T-Link TL250 module (Section [002]).
3. The static IP address of the receiver (Section [007]).
4. The static IP address of the static gateway for the LAN the T-Link TL250 is connected to in a WAN configuration (Section [008]).

NOTE: For DHCP networks, the above items are not required. Consult your network administer for information about the DHCP settings.

Remember!: If you are using a telephone line to back up communication, program the phone number you want to use as a backup or dial direction option in section [000401] 'Communication Toggle Options'. If using a PC4020 or a PC5020 [380] option 5, enables 3rd number to backup. DSC recommends that the T-Link TL250 communication be programmed to transmit first because it is faster than land line communication. If the land line communication is programmed to communicate first, then the T-Link TL250 communication will be delayed for the duration of the land line call (about 30-45 seconds). This also applies when using the phone line for backup only.

5.1 Basic Programming (PC4020 Control Panel)

NOTE: PC4020 v3.3 or higher required (Rev04B hardware).

DSC recommends changing the reporting code transmission delay from 20s to 40s on the PC4020 Steps:

Step 1 Power down the MAXSYS panel.

Step 2 Power up the MAXSYS panel. Enter installers programming ([*] + 8 + Installers Code) within the first 10 minutes of power up.

Step 3 Scroll to Diagnostics (04) and press [*].

Step 4 Scroll to Binary Programming (01) and press [*].

Step 5 Enter the address of the address location 03044 and change the value to 40 seconds (0x28).

Programming Steps:

Step 1: Program the Hex digits [CAAA] in the telephone number that will be used for T-Link TL250 communications (section [0004000000] 'Communicator + Main Items Phone Numbers').

NOTE: You must delete the [D] in the telephone number first (this is the dial tone detection).

Step 2: Program YES for 'T-Link Enabled' option, section [000401] 'Communication Toggles'.

Step 3: If using DLS communication over T-Link then program YES for 'DLS Enabled' in section [000300], 'DLS Section +DLS Toggles'.

Step 4: Program the dialer direction options for the phone number that has been programmed to send T-Link communications in section [000400XX02], where XX = telephone number 00-02 in the 'Communicator + Main Options'.

NOTE: Auto report SIA section [000401] must be enabled in order for the T-Link TL250 to communicate. The communication format must be programmed for SIA [000400XX01].

Step 5: Enter section [000406] for T-Link module programming options.

Step 6: Program the static IP address for the T-Link module in section [001]. Program 000.000.000.000 for DHCP.

Step 7: Program the subnet mask for the T-Link module in section [002]. This option will be ignored if the unit is set for DHCP.

Step 8: Program the receiver static IP address (DRL3-IP line card or the PC running The Reporter IP software) in section [007].

Step 9: If the receiver (DRL3-IP) is on a different network segment than the T-Link module, the gateway address associated with the T-Link module must be programmed in section [008]. This is an optional step; please discuss with the network administrator if this is required.

Step 10: Program the T-Link's account number in section [003].

Step 11: After all T-Link TL250 module programming is complete, you must restart the module so the programming changes will take effect. To restart the T-Link module enter the digits [55] in T-Link programming section [999] and wait 15 seconds for the module to reboot. Once complete, press the [#] key to exit T-Link TL250 programming.

Maxsys V3.5 Only:

CAAA = Receiver 0

CBBB = Receiver 1

CCCC = Receiver 2

CDDD = Receiver 3

If the panel sends events to Receiver 0, then the T-Link will perform backups automatically to IPs from Receiver 1 and Receiver 2. If the panels sends events to specific receivers then the panel will be responsible for all backup/ alternate dial functions.

NOTE: The IP Receiver addresses are programmed in the T-Link TL250.

5.2 Basic Programming (PC5020 Control Panel)

NOTE: PC5020 software version 3.2 or higher required (Rev03 hardware).

Programming Steps:

Step 1: Program the hex digits [DCAA] in the telephone number that will be used for T-Link TL250 communications (section [301] to [303], 'Telephone Phone Number Programming').

NOTE: The leading digit [D] in the telephone number for dial tone detection is already programmed.

Step 2: Program the communication format as SIA FSK format in section [350] and Auto SIA, option 3 in section [381] has to be OFF.

Step 3: Program the call direction options in section [351] to [376] for the phone number being used to communicate using T-Link TL250.

Step 4: Section [382] Option 5 'PC-Link Active' option must be ON to enable T-Link TL250 communication.

Step 5: Enter section [851] for T-Link TL250 module programming options.

NOTE: Option [5] in Section [382] must be enabled to access this section.

Step 6: Program the static IP address for the T-Link TL250 module in section [001]. Program 000.000.000.000 for DHCP.

Step 7: Program the subnet mask for the T-Link TL250 module in section [002]. This option will be ignored if the unit is set for DHCP.

Step 8: Program the static IP address of the receiver (DRL3-IP line card) in section [007].

Step 9: If the receiver (DRL3-IP) is on a different network segment than the T-Link TL250 module, the gateway address associated with the T-Link TL250 module must be programmed in section [008]. This is an optional step; please verify with the network administrator if this is required.

6.1 Advanced T-Link TL250 Programming Sections

[001] Module IP (Static IP address for the T-Link module)

Default: 192.168.000.099

Unique IP address for the module. The network administrator will provide this information. To enable DHCP program the address as 000.000.000.000.

[002] Subnet Mask

Default: 255.255.255.0

Must equal the subnet mask for the local subnet. For any single subnet, there is only one valid subnet mask; all nodes on the same subnet will use the same subnet mask. The network administrator will provide this information.

NOTE: If DHCP is enabled then this section will be ignored.

[003] T-Link Account Code

Default: FFFFFF

The account number is used by the central station to distinguish between transmitters. There is one account number programmable for the T-Link. This account number is only used when transmitting signals from inputs or internal troubles. Signals received on the PC-Link will use the panel's account number.

NOTE: The account code FFFFFF and 000000 are not valid accounts.

[004]-[005] Encryption Password (32 Hex characters max.)

Default: None

Once programmed the T-Link will use this data to encrypt and decrypt all receiver and DLS messages. The user can program a value from 1-8 bytes long in each section. To disable the encryption, program both sections with zeros. If the encryption key does not match the central station key, then the communication will FTC.

NOTE: For UL/ULC Installations, an encryption key is required.

NOTE: E-mail messages are not encrypted.

[006] T-Link Installer Code

This code is used when using the T-Link Console to remotely or locally program the T-Link.

[007] Receiver #1 IP (Static IP address for the receiver)

Default: 000 000 000 000

Program the IP address of the central station receiver.

[008] T-Link Gateway

Default: 000.000.000.000

This is the IP address of the local gateway the T-Link can use to connect with the receiver (WAN network).

The IP address of the gateway must also be a valid IP address for the local subnet.

NOTE: If DHCP is enabled then this section will be ignored.

[009] Receiver #1 T-Link Source Port Number

Default: 3060

[010] Receiver #1 T-Link Destination Port Number

Default: 3061

[011] Receiver #2 IP (Static IP address for the second receiver)

Default: 000.000.000.000

Program the IP address of the second receiver.

[012] Receiver #2 Gateway

Default: 000 000 000 000

This is the IP address of the local gateway the T-Link can use to connect with the second receiver (WAN network). The IP address of the gateway must also be a valid IP address for the local subnet.

[013] Receiver #2 T-Link Source Port Number

Default: 3065

[014] Receiver #2 T-Link Destination Port Number

Default: 3061

[015] Receiver #3 IP (Static IP address for the third receiver)

Default: 000 000 000 000

Program the IP address of the third receiver.

[016] Receiver #3 Gateway

Default: 000.000.000.000

This is the IP address of the local gateway the T-Link can use to connect with the third receiver (WAN network). The IP address of the gateway must also be a valid IP address for the local subnet.

[017] Receiver #3 T-Link Source Port Number

Default: 3066

[018] Receiver #3 T-Link Destination Port Number

Default: 3061

[019] Console Port Number

Default: 3064

[020] TFTP Port

Default: 69

Port used to do the remote flash upload.

[021] DLS Port Number

Default: 3062

[022] SA Port Number

Default: 3063

[023] T-Link Supervision Enable/Disable

Default: 0

When set to 1, the T-Link is supervised by the central station receiver.

NOTE: For UL/ULC installations, this option shall be set to 1.

[024] Receiver Failure Debounce Time

The amount of time that must elapse with no heartbeat response from the receiver before the T-Link TL2XX will generate a Receiver#1 absent condition.

NOTE: For UL installations, this option shall be set to B4h (180s). For ULC installations this option shall be set to 5Ah (90s) for Security Level 4, and to 4Bh (75s) for Security Level 5.

[025] Receiver Restoral Debounce Time

The amount of time that must elapse when the heartbeat resumes from the receiver before the T-Link TL2XX will generate a Receiver #1 restoral condition.

[026]-[027] E-mail Address 1 and 2 (64 characters max.)

Default: None

The T-Link can send alarm messages to two email addresses. The T-Link only supports SMTP to transmit e-mails in the MIME format. T-Link does not support UUENCODE message formats. T-Link does not accept any incoming messages.

NOTE: This option can only be programmed via the console software.

The following is an example of the information contained in an e-mail from the T-Link module. For more details on the SIA reporting codes, refer to the control panel Installation Manual.

From: T-Link 123456

To: recipient@address.com

Subject: T-Link v1.0.30; 123456 Event Report

Message: #6789|[Nri0/LS000]

NOTE: The account number in the subject line is the T-Link's account number. The account number in the message body is from the originator of the signal. In this example, the originator was the panel connected on the PC-Link with account number 6789. If the T-Link would have been the originator, the account number in the message body would match the account number in the subject line.

[28] E-mail From

The ‘e-mail from’ option is used for the ‘from’ field in e-mails sent out by the T-Link TL2XX. If the option is not programmed (all 0's) then the ‘from’ field of the T-Link TL2XX will look as follows:

T-Link AAAAAA where A is the account code of that T-Link TL2XX.

If the option is programmed with any ASCII character string, the ‘FROM’ field will be what is programmed in the option.

[029] DNS Server Address

Default: 000.000.000.000

In order to communicate to a T-Link via a host name program the IP address of the DNS server. The DNS lookup for the T-Link TL2xx will only work for T-Link TL2xxs with Static IP addresses (Dynamic DNS is not supported).

[030] SMTP Server Name (64 characters max.)

Default: None

In order to send e-mails to the Internet a valid outgoing e-mail server. Contact your Internet service provider or system administrator for this information.

This option can only be programmed via the Console software or the Web-browser

[031] Email Account (64 characters max.)

Default: None

Some e-mail servers will require an account name to allow outgoing messages to be sent. Contact your Internet service provider or system administrator for this information.

NOTE: This option can only be programmed via the console software or the web browser.

[032] E-mail Account Password (20 characters max.)

Default: None

Some e-mail servers will require a password and the account name to allow outgoing messages to be sent. Contact your Internet service provider or system administrator for this information

NOTE: This option can only be programmed via the Console software or the web browser.

[033] Trouble Toggle Option Section 1

Option [033] and [034] are for the trouble reporting toggles. To enable, set the specific trouble toggle option ON. To disable, set toggle to option OFF.

Toggle	Default		Description
[1]	ON	□	Network Trouble
[2]	ON	□	Invalid Account (set as FFFFFF)
[3]	ON	□	Receiver 1 Absent
[4]	ON	□	Panel Communication Trouble
[5]	OFF	□	Input Alarm
[6]	*OFF	□	FTC to Receiver 1
[7]	*OFF	□	PC5108 Absent
[8]	*OFF	□	PC5108 Tamper

Shall be ON for UL/ULC installations

[034] Trouble Toggle Option Section 2

Toggle	Default		Description
[1]	OFF	□	FTC to Receiver 2
[2]	OFF	□	Keyswitch Arm/Disarm Reporting
[3]	OFF	□	T-Link Remote Programming
[4]	OFF	□	T-Link Local Programming
[5]	OFF	□	Receiver 2 Absent
[6]-[8]		□	For Future Use

[035] PGM1 Enable/Disable

Default: 01

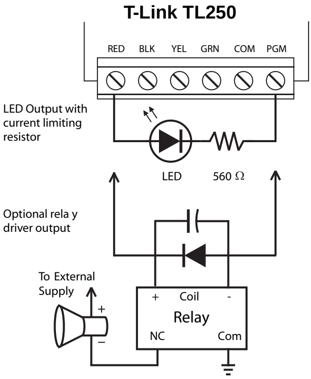
This PGM can be enabled (01) or disabled (00).

When the PGM is enabled, the output will activate when any of the trouble conditions enabled in the T-Link Trouble Toggle Options are present. It will deactivate when all the selected trouble conditions are cleared.

NOTE: If a trouble condition occurs that is not enabled in the T-Link Trouble Reporting option, the PGM will not turn on for that trouble condition nor will it be required to turn off the PGM.

PGM - The PGM1 output is dedicated for T-Link TL250 trouble indications. The PGM2 output is dedicated as an input follower for the T-Link TL250.

NOTE: For Modes 2 & 3, program option as 01.



If a control panel is not monitoring the T-Link TL250, an LED or a buzzer can be connected between this terminal and the RED terminal for trouble indication. The PGM terminal switches low from an open-collector state.

NOTE: The PGM output can sink 50mA (max.). For UL installations, use DSC RM-1 Relay Module.

[036]-[047] Digital input 1 through 12 configuration for TL250

Default: 00

Program a 2-digit code for the definition of the inputs. Select a definition from the list below.

[00] Null Input

The input is vacant. Unused inputs should be programmed as Null inputs. Any activity on this input is ignored.

[03] Instant Input

This input type will reports if the T-Link is armed, it also supports force arming. When forced armed the T-Link will arm even if the input is open. When the input is closed it is treated as a normal instant input. SIA Reporting Code: BA/BH.

[08] Standard 24-hr Fire Input

When this input is violated, the panel immediately communicates to the central station. SIA Reporting Code: FA/FH.

[11] Standard 24-hr Burglary

When this input is violated, the panel immediately communicates to the central station. SIA Reporting Code: BA/BH.

[16] 24-hr Panic Input

If this input is violated, when the system is armed or disarmed, the panel reports to the central station. SIA Reporting Code: PA/PH.

[21] 24-hr Tamper

When this input is violated, the panel immediately communicates to the central station. SIA Reporting Code: TA/TH.

[23] Maintained Keyswitch Arm Input (Input 2 Only)

When this input is violated, the system will arm. When this input is secured, the system will disarm. All instant type inputs have force arming support.

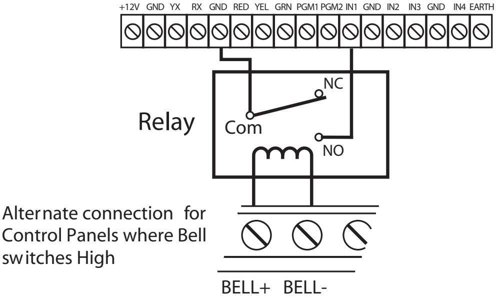
SIA Reporting Code: CS/OS.

[99] 24-hr Bell Follower Input

Input 1 can only be programmed to follow the Bell output for burg/fire monitoring. Connect Input 1 to the Control Panel Bell+ output.

This will disable signal sending when arm and disarm squawks are generated. See Options [062] through [065].

Mode 1 - Bell Follower Operation


+12V GND YX RX GND RED YEL GRN PGM1 PGM2 IN1 GND IN2 IN3 GND IN4 EARTH
Relay
NC
Com
NO
Alternate connection for Control Panels where Bell switches High
BELL+ BELL-

[048] Input 1 Configuration

Default: 0

Set to 0 for normally open inputs.

Set to 1 for normally closed inputs.

NOTE: Select this option when Normally Closed (NC) detection devices or contacts are being used on Input 1.

[049] Input 2 to 4 Configuration

Default: 0

Set to 0 for normally open contacts.

Set to 1 for normally close contacts.

[050]-[061] SIA Reporting Input

If '00' is entered, central station reporting is disabled. All other actions for PGM outputs and status are still activated.

If 'FF' is entered, default reporting code is enabled using the input definitions, with the hardcoded input number.

If anything between 01 and 99 is programmed, the hardcoded input number will be replaced by the programmed value.

Alarm Reporting Codes, Inputs 1-12

Default:			Default:		
FF	|___|___|	Input 1 Alarm	FF	|___|___|	Input 7 Alarm
FF	|___|___|	Input 2 Alarm	FF	|___|___|	Input 8 Alarm
FF	|___|___|	Input 3 Alarm	FF	|___|___|	Input 9 Alarm
FF	|___|___|	Input 4 Alarm	FF	|___|___|	Input 10 Alarm
FF	|___|___|	Input 5 Alarm	FF	|___|___|	Input 11 Alarm
FF	|___|___|	Input 6 Alarm	FF	|___|___|	Input 12 Alarm

[062] Fire On Time

Default: 05

The Bell Pulse On Time is used with Digital Input#1 when configured for Bell Follower mode. The Bell Pulse On/Off Time is the time of the pulse width. This option is programmed in hex times 100 milliseconds.

[063] Fire Off Time

Default: 05

The Bell Steady On Time is used with Digital Input #1 when configured for Bell Follower mode. This is the minimum time in 100ms increments that the bell must be active/sounding before it will be considered a steady on state and generate the Burglary Alarms. This option is programmed in hex times 100 milliseconds.

[064] Restoral Delay Time

The Restoral Delay Time is used with Digital Input#1 when configured for Bell Follower mode. It is the minimum time that the bell must be inactive before it will be considered a Fire/Burglary Restoral.

[065] Fire Pulse Count

The Fire Pulse Count is used with Digital Input #1 when configured for Bell Follower mode. The pulsed count will be the minimum number of pulses (high and low forming 1 cycle) before the T-Link will consider it an alarm state.

[066] SIA ACK Time

The SIA ACK Time option is the maximum wait time for a response from a receiver for any messages sent to the receiver.

[901] Current T-Link IP Address

The Current T-Link IP Address is a read-only option. If this option is selected through the panel programming, the T-Link TL2XX will respond with the current IP address of the T-Link TL2XX and display it on the keypad for the user.

Sect.	Description	Default Value
001	T-Link IP Address	192.168.0.99
002	T-Link Subnet Mask	255.255.255.0
003	T-Link Account Code	FFFFFFFF
004	Receiver Encryption Password	0000000000000000
005	Receiver Encryption Password	0000000000000000
006	Installer Code[i]	CAFE
007	Primary Receiver IP Address	0.0.0.0
008	Primary Receiver Gateway IP Address	0.0.0.0
009	Receiver Local Port	3060
010	Receiver Remote Port	3061
011	Secondary Receiver IP Address	0.0.0.0
012	Secondary Receiver Gateway IP Address	0.0.0.0
013	Receiver#2 Local Port	3065
014	Receiver#2 Remote Port	3061
015	Receiver 3 IP Address	0.0.0.0
016	Receiver 3 Gateway IP Address	0.0.0.0
017	Receiver#3 Local Port	3066
018	Receiver#3 Remote Port	3061
019	Console Port	3064

Sect.	Description	Default Value
020	TFTP port	69
021	DLS Port	3062
022	SA Port	3063
023	Supervision Enable (UL/ULC option must be set to 1)	0
024	Receiver Failure Debounce Time (UL = B4, ULC Security Level 4 = 5A, Security Level 5 = 4B)	0x0078
025	Receiver Restoral Debounce Time	0x003C
026	E-Mail Address 1	Null
027	E-Mail Address 2	Null
028	E-Mail From	Null
029	DNS Server IP Address	0.0.0.0
030	SMTP Server	Null
031	Email Account	Null
032	Email Password	Null
033	T-Link Trouble Reporting	See Troubles
034	T-Link Trouble Reporting	See Troubles
035	T-Link Programmable Output #1	Disabled
036	Digital Input 01 Definition	00 (Disabled)
037	Digital Input 02 Definition	00 (Disabled)
038	Digital Input 03 Definition	00 (Disabled)
039	Digital Input 04 Definition	00 (Disabled)
040	Digital Input 05 Definition	00 (Disabled)

Sect.	Description	Default Value
041	Digital Input 06 Definition □□	00 (Disabled)
042	Digital Input 07 Definition □□	00 (Disabled)
043	Digital Input 08 Definition □□	00 (Disabled)
044	Digital Input 09 Definition □□	00 (Disabled)
045	Digital Input 10 Definition □□	00 (Disabled)
046	Digital Input 11 Definition □□	00 (Disabled)
047	Digital Input 12 Definition □□	00 (Disabled)
048	Digital Input 01 configuration: N.C. or N.O. □	00 (N.O.)
049	Digital Input 02-04 configuration: N.C. or N.O. □	00 (N.O.)
050	Digital Input 01 SIA Reporting Code □□	0xFF
051	Digital Input 02 SIA Reporting Code □□	0xFF
052	Digital Input 03 SIA Reporting Code □□	0xFF
053	Digital Input 04 SIA Reporting Code □□	0xFF
054	Digital Input 05 SIA Reporting Code □□	0xFF
055	Digital Input 06 SIA Reporting Code □□	0xFF
056	Digital Input 07 SIA Reporting Code □□	0xFF
057	Digital Input 08 SIA Reporting Code □□	0xFF
058	Digital Input 09 SIA Reporting Code □□	0xFF
059	Digital Input 10 SIA Reporting Code □□	0xFF

Sect.	Description	Default Value
060	Digital Input 11 SIA Reporting Code └───┴───┘	0xFF
061	Digital Input 12 SIA Reporting Code └───┴───┘	0xFF
062	Fire On Time └───┴───┘	0x05
063	Fire Off Time └───┴───┘	0x05
064	Restoral Delay Time └───┴───┘	0x64
065	Fire Pulse Count └───┴───┘	0x03
066	SIA ACK Time └───┴───┘	0x02
901	Current T-Link IP Address └───┴───┴───┘ └───┴───┴───┘ └───┴───┴───┘ └───┴───┴───┘	

Console

A PC application program which can connect to the receiver and provide Diagnostic and programming abilities to the user.

DHCP

***D**ynamic **H**ost **C**onfiguration **P**rotocol*, a protocol for assigning dynamic IP addresses. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the server keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

Encryption

The translation of data into a secret code usually based on a key. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt.

Ethernet

A local-area network (LAN) protocol developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. A newer version of Ethernet, called 100BaseT (or Fast Ethernet), supports data transfer rates of 100 Mbps. The newest version, Gigabit Ethernet, supports data rates of 1 Gigabit (1,000 Megabits) per second.

IEEE

Abbreviation of ***I**nstitute of **E**lectrical and **E**lectronics **E**ngineers*, pronounced I-triple-E. Founded in 1963, the IEEE is an organization composed of engineers, scientists, and students. The IEEE is best known for developing standards for the computer and electronics industry.

Intranet

A network based on TCP/IP protocols belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization.

IP

Abbreviation of ***I**nternet **P**rotocol*, pronounced as two separate letters. IP specifies the format of packets, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two devices so that they can send messages back and forth for a period of time.

IP Address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

LAN

A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide area network (WAN).

MAC

Short for ***M**edia **A**ccess **C**ontrol* address, a hardware address that uniquely identifies each device of a network. The address is not programmable by the user and the manufacturer of the device must register with IEEE before receiving an assigned group of addresses.

Mime

***M**ultipurpose **I**nternet **M**ail **E**xtensions*, a specification for formatting non-ASCII messages so that they can be sent over the internet.

Network

Two or more computer systems connected together.

Packet

A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data.

Subnet

A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. Dividing a network into subnets is useful for both security and performance reasons.

Subnet Mask

A mask used to determine to what subnet an **IP address** belongs.

TCP

Abbreviation of ***T**ransport **C**ontrol **P**rotocol*, and pronounced as separate letters. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two devices to establish a connection and exchange data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

TFTP

Trivial File Transfer Protocol. A version of the FTP protocol that has no directory or password capability. Most commonly used protocol to upgrade firmware of network devices.

UDP

User Datagram Protocol. A TCP/IP protocol which allows for connectionless communications between two network hosts. Retries are not handled and packet delivery is not guaranteed. Packets may also arrive out of sequence.

WAN

A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

Computers connected to a wide area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.

Appendix A: T-Link Functionality & Troubleshooting

To simplify bench testing and increase diagnostic ability, it is often beneficial to connect the T-Link TL250 and the receiver directly to each other, using an Ethernet crossover cable (see Section *A.2 "Making an Ethernet Crossover Cable"*). The diagnostic information for use with a crossover cable is outlined in this section.

Upon T-Link TL250 power-up (without the Ethernet cable connected), LED2 will blink periodically, approximately once every 12 seconds. This represents the T-Link TL250 attempting to send a connection request to the receiver. The TL250 will try to connect to the receiver until it succeeds.

A.1 Troubleshooting

There are 3 LEDs on the board to indicate connection and traffic status:

- LINK STATUS
- ACTIVITY STATUS
- SPEED STATUS LEDs.

LK LED = Link Status (ON = Ethernet Present OFF = Ethernet Absent)

ACT = Activity Status (Displays Network Traffic RX/TX)

SPD LED = Speed Status (ON = 100Mbps Connection OFF = 10Mbps Connection)

SPD LED will always display the connection speed once connected to the network.

Both **ACT** and **LK LED** are normally OFF in their default state after power-up (i.e. when no Ethernet cable is connected, and there are no packets being transmitted or received, respectively).

When connected to the network, **LK LED** will turn on.

When a packet is transmitted and/or received, **ACT** will blink.

A.2 Making an Ethernet Crossover Cable

An Ethernet crossover cable can be made by taking a standard Ethernet cable (which will have wires attached to pins 1, 2, 3 and 6 only on the 8 pin RJ-45 connector) and swapping pin 1 with pin 3, and also swapping pin 2 with pin 6, on one end of the cable only. This effectively reverses the transmit and receive pairs, and allows two hosts to communicate without the use of a network hub.

A.3 Call Direction

The call direction options of the panels are compatible with the T-Link module. For example, if telephone number one is programmed for the T-Link and network communication is lost, the panel will use the backup telephone number to send the information to the central station. The communication format is telephone number-specific and therefore the land line communication format can be different from the T-Link's SIA format.

A.4 Port Usage Table

NOTE: Please confirm with the network administrator that the following ports are locked open and that the SG-DRL3-IP has network access for all required network segments.

Description		Default Port #	Programming Location to Change
T-Link TL250	T-Link Source Port	3060	Section [009] T-Link options from Keypad
	T-Link Destination Port	3061	Section [010] T-Link options from Keypad
SG-DRL3-IP	T-Link Port	3061	Section [0B] [0C] from Console S/W
	DLS Port	3062	Section [0D] [0E] from Console S/W
	SA Port	3063	Section [11] [12] from Console S/W
	Console S/W Port	3064	Section [14] [15] from Console S/W
DLS2002	DLS Port	3062	Modem Configuration Options
DLS SA	SA Port	3063	Modem Configuration Options
Console	Console Port	3064	
T-Link Console TFTP	Firmware Upgrade	69	

A.5 Integrated Call Directions

The T-Link features a built-in call direction that will allow signals to be sent to active receivers as well as a local LAN logging application.

The T-Link has a choice of 3 receivers when transmitting signals. Receiver 1, Receiver 2 and Receiver 3. Should the communications be lost to Receiver 1, the T-Link will generate a local trouble and send the trouble to the appropriate receiver. The loss of Receiver 2 or 3 does not generate any signal since they are not supervised.

The panel can direct to which receiver the signal will be sent. If a Receiver is lost, the T-Link TL250 will route the alarm to the backup receiver (if programmed). Receiver 3 will be used as a local logging. Any signal sent to either Receiver 1 or Receiver 2 will also be sent to Receiver 3. Once the connections has been restablished to Receiver 1 the T-link will resume transmission to it.

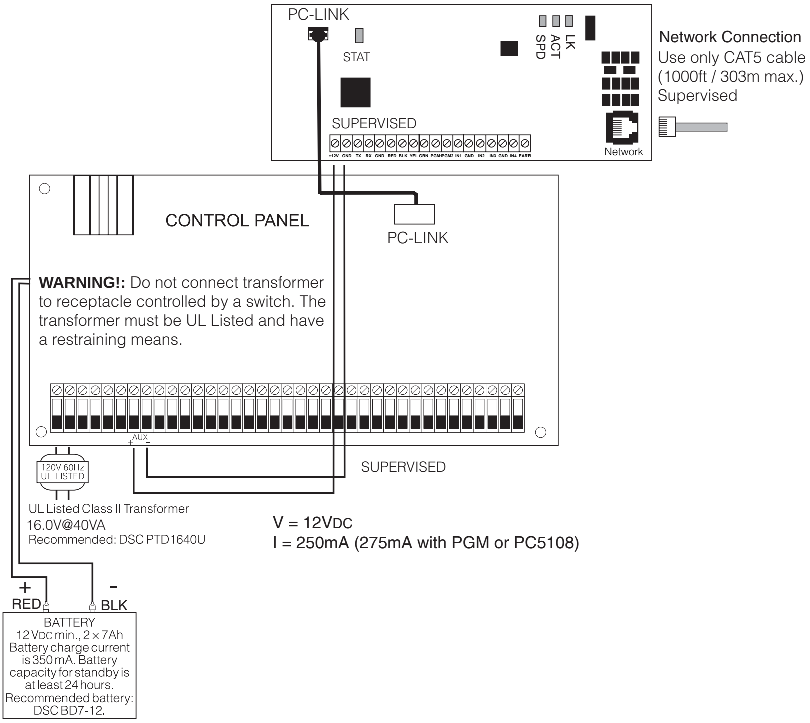
NOTE: If Receiver 1, 2 or 3 is not programmed, T-Link will not attempt to report to the receiver.

B.1 Standard Connection with PC4020(CF)/PC5020(CF)

CAUTION! *All circuits are supervised and power limited. Refer to Battery Lead and AC Power Lead Routing for UL Listed Commercial Fire Systems diagram for wire routing. Do not route any wiring over the circuit boards. Maintain at least 1" (25.4mm) separation between circuit board and wiring.*

A minimum of 1/4" (7mm) separation must be maintained at all points between non power limited wiring and power limited wiring.

Refer to your control panel Installation Manual for any additional information.

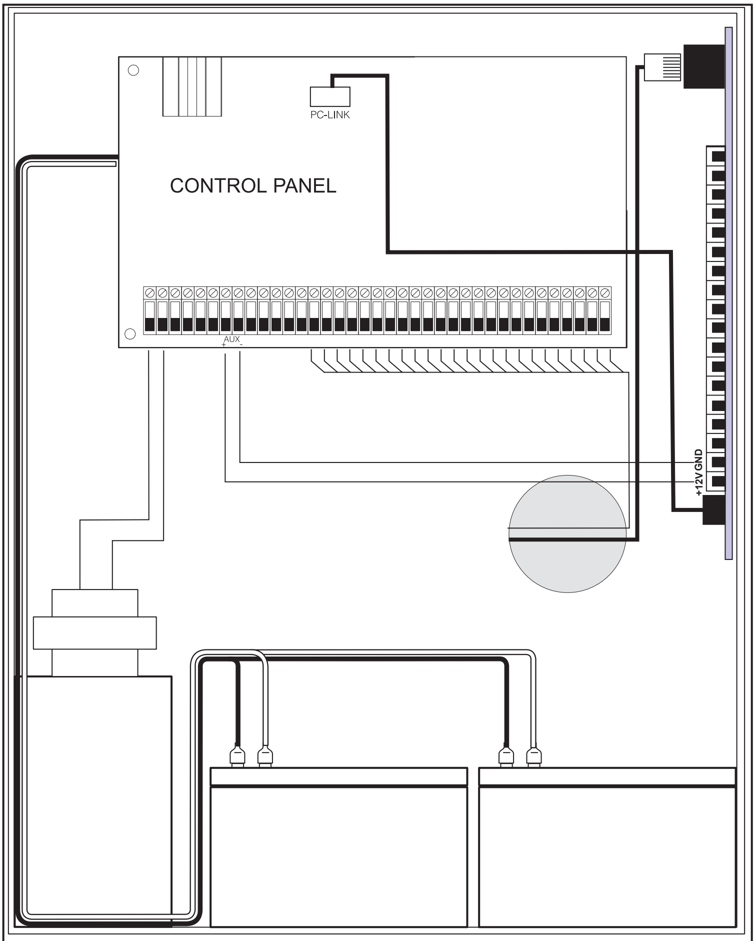

PC-LINK
STAT
SPD
ACT
LK
SUPERVISED
+12V GND TX RX GND RED BLK YEL GRN PGM1 PGM2 IN1 GND IN2 IN3 GND IN4 EARTH
Network
Network Connection
Use only CAT5 cable
(1000ft / 303m max.)
Supervised
CONTROL PANEL
PC-LINK
WARNING!: Do not connect transformer to receptacle controlled by a switch. The transformer must be UL Listed and have a restraining means.
AUX
+ −
120V 60Hz
UL LISTED
SUPERVISED
UL Listed Class II Transformer
16.0V@40VA
Recommended: DSC PTD1640U
V = 12VDC
I = 250mA (275mA with PGM or PC5108)
+
RED
−
BLK
BATTERY
12 VDC min., 2 × 7Ah
Battery charge current is 350 mA. Battery capacity for standby is at least 24 hours.
Recommended battery: DSC BD7-12.

Wiring T-Link to a DSC Compatible Control Panel

- Secure the T-Link module to the side of the cabinet using the supplied standoffs.
- With both AC and battery disconnected removed from the DSC control panel, wire the T-Link to the panel using 4 wires from the PC-Link of the panel to the "PANEL" connector on the T-Link.
- Wire the panel's AUX + and - to 12VDC and GND terminals of T-Link.
- Apply AC and DC to the main control panel. Both the T-Link and the panel should power up.
- Do the necessary programming that is required.

NOTE: If a Bell/Siren is not going to be used, wire the Bell/Siren terminals on the panel with a 1000 ohm resistor. For Commercial Fire installation, when a bell/siren is used in the application, it should be connected to the DSC module PC4702BP. Please refer to the PC4020 Installation Manual. The keypad or any other accessory connected to the Combus shall be connected within 3 feet / 0.9 m and in conduit.

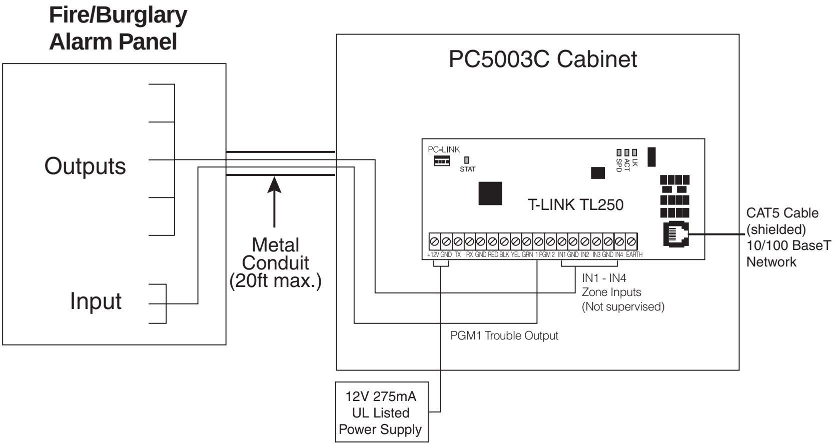
B.2 Battery Lead and AC Power Lead Routing for UL Listed Commercial Fire Systems



INSTALL BATTERY AND AC WIRING AS SHOWN ABOVE
IMPORTANT: A minimum ¼" (7mm) separation must be maintained at all points between battery/primary AC wiring and all other wiring and connections.

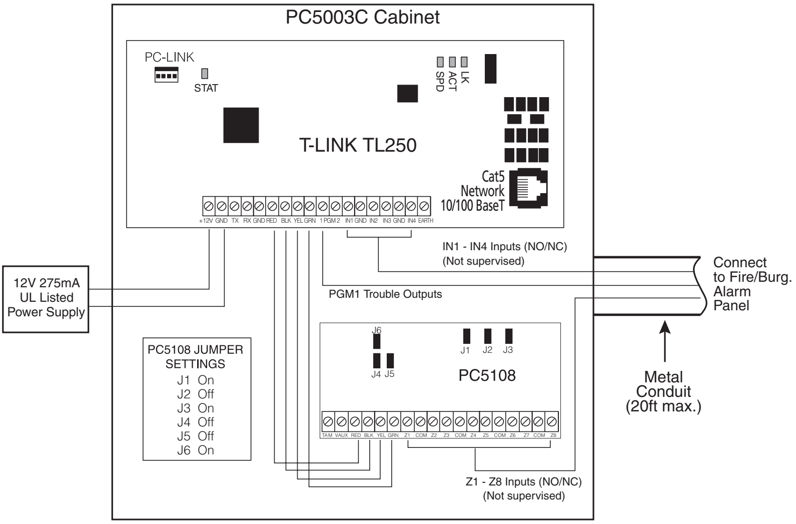
T-Link board must be mounted on the side of the cabinet. Refer to the mounting instructions in the associated Installation Manual.

B.3 Mode 2 Configuration



B.4 Input Expander (Mode 3 Configuration)

To expand from the 4-zone inputs a PC5108 must be connected to the T-Link. Connect the Keybus from the PC5108 to the Keybus of the T-Link TL250. Any devices that require 12VDC, motion detectors, glassbreak detectors, etc., will require an external 12VDC power supply.



Appendix C: T-Link Events

T-Link events sent to the central station.

Description	SIA Event Code
Panel Absent	ET0001
Panel Restored	ER0001
FTC1 Alarm	YC0001
FTC1 Restoral	YK0001
FTC2 Alarm	YC0002
FTC2 Restoral	YK0002
PC5108 Tamper Alarm	ES0000
PC5108 Tamper Restoral	EJ0000
PC5108 Absent	ET0002
PC5108 Restored	ER0002
Keyswitch Arm	CS0000
Keyswitch Disarm	OS0000
Remote Programming Start	RB0000
Remote Programming End	RS0000
Local Programming Start	LB0000
Local Programming End	LS0000
Internal Comm. Error	YC0000

Appendix D: T-Link TL250 Compatibility Chart

Compatible DSC Control Panels	
MAXSYS PC4020	• Software V3.31 or higher • Hardware Rev 04B
Power864 PC5020	• Software V3.2 or higher • Hardware Rev 03
TCP/IP Communicator	
T-Link TL250	• 10/100 BaseT • TCP/IP communication module • Static or DHCP IP configurable • Additional zone inputs using PC5108 • Program locally using PowerSeries keypad.
TCP/IP Communication Routing / Receiver	
SG-DRL3-IP V1.0 *	• Supports 1024 accounts, of which, up to 512 can be supervised • Static IP required per DRL3-IP
Downloading Software	
DLS2002	• Required • CD from distributor or free download from dsc.com with a valid password
Maxsys PC4020 V3.3 (with TCP/IP support) Driver Pack	• Required • Free download from dsc.com with a valid password
Power864 PC5020 V3.2 DLS-3 Driver	• Required • Free download from dsc.com with a valid password
System Administration Software	
DLS-3 SA V1.3	• Required • Kit with modem or PC4401 from distributor
DLS-3 SA V1.3 Service Pack 1 for Maxsys V3.31 support	• Required • Included in the kit or free download from dscsec.com/dls3drivers.htm
DLS-3 SA V1.3 Service Pack 2 for Power864 v3.2 support	• Required • Included in the kit or free download from dscsec.com/dls3drivers.htm
***NOTE:** The DLS software could be used with UL Listed installations only when a service personnel is on the site.	

Installation Instructions

Important

The following requirements for installation of CAT5 ethernet cable must be observed for correct operation of connected equipment.

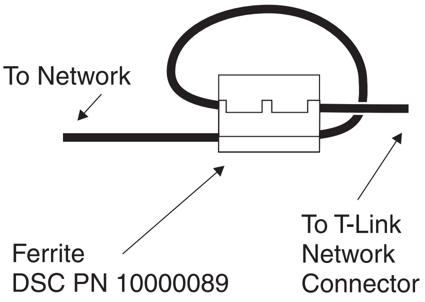
Do **NOT** strip off cable sheathing more than required for proper termination.
Do **NOT** kink or knot cable.
Do **NOT** crush cable with cable ties.
Do **NOT** splice cable.
Do **NOT** bend cable at right angles or make any other sharp bends.

Note: All cable bends must have a minimum 2" (50mm.) radius.

Do **NOT** untwist CAT5 pairs more than ½” (12mm.)
Do **NOT** exceed maximum 6” (150mm.) from center of ferrite to T-Link Network Connector

INSTALLATION of CAT-5 Ethernet Cable

CAT5 Ethernet Cable



Note:

Install the Ferrite inside the control panel as close to the T-Link network connector as allowable.

6” (150 mm.) max from center of ferrite to the network connector).

Limited Warranty

Digital Security Controls warrants the original purchaser that for a period of twelve months from the date of purchase, the product shall be free of defects in materials and workmanship under normal use. During the warranty period, Digital Security Controls shall, at its option, repair or replace any defective product upon return of the product to its factory, at no charge for labour and materials. Any replacement and/or repaired parts are warranted for the remainder of the original warranty or ninety (90) days, whichever is longer. The original purchaser must promptly notify Digital Security Controls in writing that there is defect in material or workmanship, such written notice to be received in all events prior to expiration of the warranty period. There is absolutely no warranty on software and all software products are sold as a user license under the terms of the software license agreement included with the product. The Customer assumes all responsibility for the proper selection, installation, operation and maintenance of any products purchased from DSC. Custom products are only warranted to the extent that they do not function upon delivery. In such cases, DSC can replace or credit at its option.

International Warranty

The warranty for international customers is the same as for any customer within Canada and the United States, with the exception that Digital Security Controls shall not be responsible for any customs fees, taxes, or VAT that may be due.

Warranty Procedure

To obtain service under this warranty, please return the item(s) in question to the point of purchase. All authorized distributors and dealers have a warranty program. Anyone returning goods to Digital Security Controls must first obtain an authorization number. Digital Security Controls will not accept any shipment whatsoever for which prior authorization has not been obtained.

Conditions to Void Warranty

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:

- damage incurred in shipping or handling;
- damage caused by disaster such as fire, flood, wind, earthquake or lightning;
- damage due to causes beyond the control of Digital Security Controls such as excessive voltage, mechanical shock or water damage;
- damage caused by unauthorized attachment, alterations, modifications or foreign objects;
- damage caused by peripherals (unless such peripherals were supplied by Digital Security Controls);
- defects caused by failure to provide a suitable installation environment for the products;
- damage caused by use of the products for purposes other than those for which it was designed;
- damage from improper maintenance;
- damage arising out of any other abuse, mishandling or improper application of the products.

Items Not Covered by Warranty

In addition to the items which void the Warranty, the following items shall not be covered by Warranty: (i) freight cost to the repair centre; (ii) products which are not identified with DSC's product label and lot number or serial number; (iii) products disassembled or repaired in such a manner as to adversely affect performance or prevent adequate inspection or testing to verify any warranty claim. Access cards or tags returned for replacement under warranty will be credited or replaced at DSC's option. Products not covered by this warranty, or otherwise out of warranty due to age, misuse, or damage shall be evaluated, and a repair estimate shall be provided. No repair work will be performed until a valid purchase order is received from the Customer and a Return Merchandise Authorisation number (RMA) is issued by DSC's Customer Service.

Digital Security Controls' liability for failure to repair the product under this warranty after a reasonable number of attempts will be limited to a replacement of the product, as the exclusive remedy for breach of warranty. Under no circumstances shall Digital Security Controls be liable for any special, incidental, or consequential damages based upon breach of warranty, breach of contract, negligence, strict liability, or any other legal theory. Such damages include, but are not limited to, loss of profits, loss of the product or any associated equipment, cost of capital, cost of substitute or replacement equipment, facilities or services, down time, purchaser's time, the claims of third parties, including customers, and injury to property. The laws of some jurisdictions limit or do not allow the disclaimer of consequential damages. If the laws of such a jurisdiction apply to any claim by or against DSC, the limitations and disclaimers contained here shall be to the greatest extent permitted by law. Some states do not allow the exclusion or limitation of incidental or consequential damages, so that the above may not apply to you.

Disclaimer of Warranties

This warranty contains the entire warranty and shall be in lieu of any and all other warranties, whether expressed or implied (including all implied warranties of merchantability or fitness for a particular purpose) and of all other obligations or liabilities on the part of Digital Security Controls Digital Security Controls neither assumes responsibility for nor authorizes any other person purporting to act on its behalf to modify or to change this warranty, nor to assume for it any other warranty or liability concerning this product.

This disclaimer of warranties and limited warranty are governed by the laws of the province of Ontario, Canada.

WARNING: Digital Security Controls recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.

Out of Warranty Repairs

Digital Security Controls will at its option repair or replace out-of-warranty products which are returned to its factory according to the following conditions. Anyone returning goods to Digital Security Controls must first obtain an authorization number. Digital Security Controls will not accept any shipment whatsoever for which prior authorization has not been obtained.

Products which Digital Security Controls determines to be repairable will be repaired and returned. A set fee which Digital Security Controls has predetermined and which may be revised from time to time, will be charged for each unit repaired.

FCC Compliance Statement

CAUTION: Changes or modifications not expressly approved by the manufacturer could void your authority to use this equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

The user may find the following booklet prepared by the FCC useful: “How to Identify and Resolve Radio/Television Interference Problems”. This booklet is available from the U.S. Government Printing Office, Washington D.C. 20402, Stock # 004-000-00345-4.

DSC®

Toronto, Canada • **www.dsc.com**
Tech Support: 1-800-387-3630 (Canada & US) or 905-760-3036
Printed in Canada

29034631R003