T-Link TL250/TL300
Network Internet
Alarm Communicator

DSC® (UL) (ULC) C€ Installation Manual

Software Version 1.20

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

Section 1: Introduction

T-Link TL250/TL300

The T-Link TL250/300 modules are network internet communicators that send alarm system information to a central station receiver. The module 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.

T-Link TL300

The T-Link TL300 connects directly to the telephone output of a control panel and simulates a telephone connection, providing a TCP/IP connection that sends predefined Contact ID codes to the central station. The T-Link TL300 on-board zones can be used as in mode 2 (4-zone stand-alone) and mode 3 (12-zone stand-alone). Modes 1 and 5 are not supported.

Software Version 1.0

• Supports TL250 and Modes 1, 2, 3 and 4 only.

Software Version 1.10

• Supports TL250, includes Version 1.0 options and Mode 5, TL250 DVACS panel conversion (Canada only). Corresponding version numbers for SG DRL3-IP and T-Link Console are required to ensure compatibility (i.e., SG DRL3-IP v1.10 and T-Link Console v1.10 are required for corresponding T-Link TL250 v1.10).

NOTE: For DVACS mode an SG-DRL3-IP v1.10 receiver line card is required to communicate with the T-Link TL250 v1.10 or higher.

• Account code extended from 6 to 10 digits.

Software Version 1.20

• Supports TL250 and TL300 and all Version 1.10 options.
• Supports new zone type **'98'** *Panel Absent.*
• Supports basic programming from an LCD 5500 Keypad.
• Default Installer code has changed from CAFE to 5555 for this software version

1.1 Operating Modes

Mode 1: Bell Follower (TL250 only)

In Mode 1, the T-Link TL250 monitors the Bell Output of a 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 section 3 for details

Refer to the appropriate control panel *Installation Manual*.

NOTE: Do not use Mode 1 for UL or ULC listed installations.

Mode 2: 4-Zone Panel (TL250 and TL300)

In Mode 2, the system is configured for 4-zone, stand alone operation. Refer to section 4.1 for details.

Mode 3: 12-Zone Panel (TL250 and TL300)

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 section 4.2 for 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 (TL250 only)

In standard mode, the system is configured as a communicator with a compatible DSC alarm panel: Models PC4020, PC4020CF, PC5020 or PC5020CF. Refer to section 5 for details.

Mode 5: DVACS®* Mode (V1.10 or later)(TL250 only)

In DVACS mode, the system is configured as a communicator with a compatible DVACS alarm panel. Refer to section 6 for details. Refer to appendix C for a list of compatible DVACS panels and modules.

NOTE: T-Link TL250 zone events are transmitted using the standard T-Link SIA protocol. DVACS generated events are transmitted using the DVACS protocol.

NOTE: DVACS Mode 5 is used in ULC listed installations.

* DVACS is a registered trademark of Electro Arts Ltd. Scarborough Ontario, Canada

1.2   Specifications/Requirements

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).

Specifications
Input Voltage: 12 VDC
Input Current: T-LINK TL250 Max current draw: 275mA   T-LINK TL300 Max current draw: 360mA
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, TCP/IP for Console and DLS communications
Input Protocols: PC-Link (SIA format), DVACS (V1.10 and higher), Contact ID protocol. (TL300 Only)
Digital Inputs: 4-digital inputs (can be increased to 12 using the PC5108)
Connectors: 4-pin header for the PC-Link and RJ-45 for Ethernet, DVACS adaptor (DVACS kit only)
Programming: Panel keypad, console on the RS232 or remote T-Link console.
Network: Ethernet LAN/WAN 10 BaseT or 10/100 BaseT
E-mail: sends alarm messages to maximum 2 E-mail addresses (**NOT** available for DVACS installations)
Downloading Support for DSC Panels: DLS-3 and/or System Administrator software
Multiple Central Stations: primary and backup via phone line* (**NOT** available for DVACS installations).
Call Direction Options: primary or backup communicator using panel call direction (**NOT** available for DVACS installations).
Approval Listings: FCC, IC, CE UL (Grade of Service AA, Encrypted Line Security) ULC (Signal Channel Security Level 4/5)

*NOTE:This manual shall be used with the Installation Manual of the associated Alarm Controller for installation.

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.

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

NOTE:This equipment (T-Link TL250) shall be installed and used within an environment that provides the POLLUTION DEGREE MAX 2 and OVERVOLTAGES CATEGORY II NON-HAZARDOUS LOCATIONS, indoor only. The equipment must be FIXED and permanently connected, and is intended to be installed by SERVICE PERSONS (i.e., having the appropriate technical training and experience necessary to be aware of hazards which that person may be exposed to in performing the task, and of measures to minimize the risks to that person or other persons).

CAUTION

Ethernet communication lines must be connected to an approved (acceptable to local authorities) type NID (Network Interface Device) before leaving the premises (e.g., UL installations, UL60950 Listed NID).

Section 2: Quick Start

2.1 Installation

1. Determine the Operating Mode Required

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

2. Determine the Mounting Location

Select a mounting location in a dry, protected area at least 30 cm. away from physical contact with any person. Refer to page 34, appendix C, 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 module.
- Shielded wire is not necessary unless wires are run in an area that may present excessive RF noise or interference.
- Refer to section 9, Programming Descriptions, section [36] for zone wiring details.

3. Route Wiring to Mounting Location

Route wiring from the hard wired zones or control panel as required.

NOTE: Route wiring through conduit to a junction box if possible.

4. Mount the T-Link TL250/300 Panel

2.2 Testing

Mode 4, Standard Mode: Ensure the panel is programmed to use the T-Link TL250 in accordance with the settings outlined in section 8, 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: Ensure the T-Link is programmed in accordance with the settings outlined in Sections 9, 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.

Modes 2, 3 and 5 (DVACS): Simulate Inputs violations in accordance with the settings outlined in Sections 9, Programming Descriptions. Verify that the T-Link TL250 transmits the events to the central station.

TL300 Simulated Phone: Ensure the T-Link TL300 Input 1 is programmed in accordance with the TL300 settings outlined in Sections 9, Programming Descriptions. Simulate Burglar and Fire Zone violation on the alarm panel. Verify that the T-Link TL300 transmits the associated Contact ID code to the central station.

2.3 Resetting to Factory Defaults

Hardware Defaults (all modes)
- Remove Power from the T-Link TL250/TL300; 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 T-LINK TL250/TL300 for approximately 20 seconds
- Reconnect all original wiring and reapply power to the T-Link TL250/TL300.
- 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.

Mode 4:

In mode 4, the T-Link can be Defaulted through the panel keypad:
- Enter section 999 of the T-Link TL250
- Enter 00 to default the unit to factory settings
- Enter 55 to restart the unit.

2.4 LCD 5500 Programming

All Modes (Software version 1.2 only)
Local programming of basic options can be done through a standard DSC Power LCD keypad. Connect the keypad on the T-Link Keybus terminals. Access to programming mode uses the same code as the console (default is '5555').

NOTE:Programming mode access can be done only on power up for 30 seconds, and only if the reset to factory default is not activated.

- Access the Installer mode using [*][8], followed by the installer code.

NOTE:The [*] and [#] keys are not supported to re-enter installer code in the event of an incorrect entry. All keys will be ignored if the correct sequence following [*][8] is not entered.

- Four Programming Sections are available and will be displayed in the sequence indicated below. See section 9 for details

      [001] T-Link IP Address:
      |___|___|___|.|___|___|___|.|___|___|___|.|___|___|___|

      [003] T-Link Account Code
      |___|___|___|___|___|___|___|___|___|___|

      [007] Primary Receiver IP Address
      |___|___|___|.|___|___|___|.|___|___|___|.|___|___|___|

      [007] Primary Receiver Gateway IP Address
      |___|___|___|.|___|___|___|.|___|___|___|.|___|___|___|

When programming is completed, press the "#" key to save changes and exit programming mode. A 2-minute timing delay begins when entering the programming mode. At the end of the timing delay T-Link will exit program mode and save the changes made regardless of where the programmer is in the programming sequence.

- 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.

Section 3: Bell Follower Installation (Mode1)

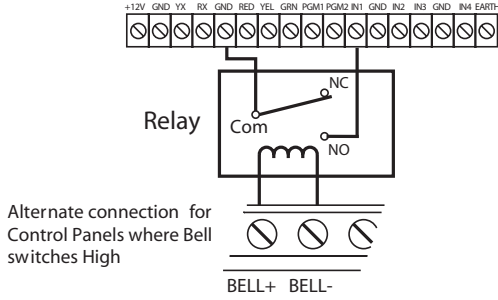## 3.1 Setup and Installation

3.1.1 Bell Follower Installation (Mode 1)

Install the T-Link TL250 in a DSC enclosure (model PC5003C) when used in a Bell Follower configuration. Refer to section [036][99].

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

NOTE: Bell Follower mode can not be used in UL or ULC listed installations.

Refer to options [062] through [065].

Section 4: Stand-alone Installation (Modes 2&3)

Install the T-Link TL250 in a DSC enclosure (model PC5003C) when used in a stand-alone configuration or with the PC5108 module.

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

NOTE: For UL Listed installations, the power supply used must be UL Listed for the application.

4.1   Stand alone Mode 2 Configuration
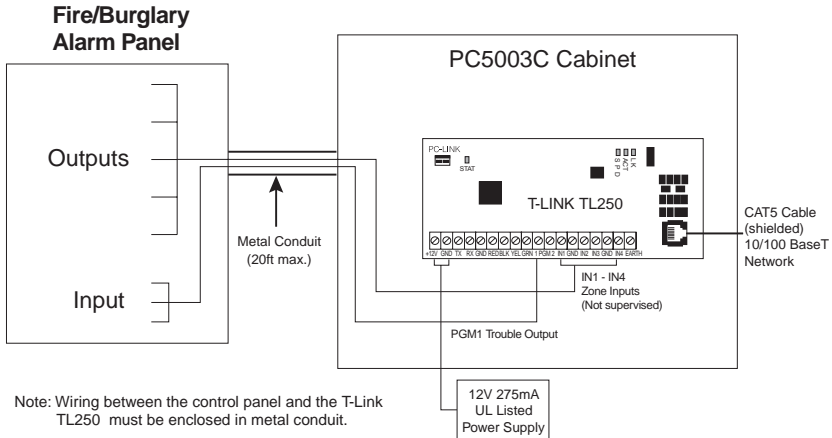
4.2   Input Expander (Mode 3 Configuration)

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, glass break detectors, etc., will require an external 12VDC power supply.
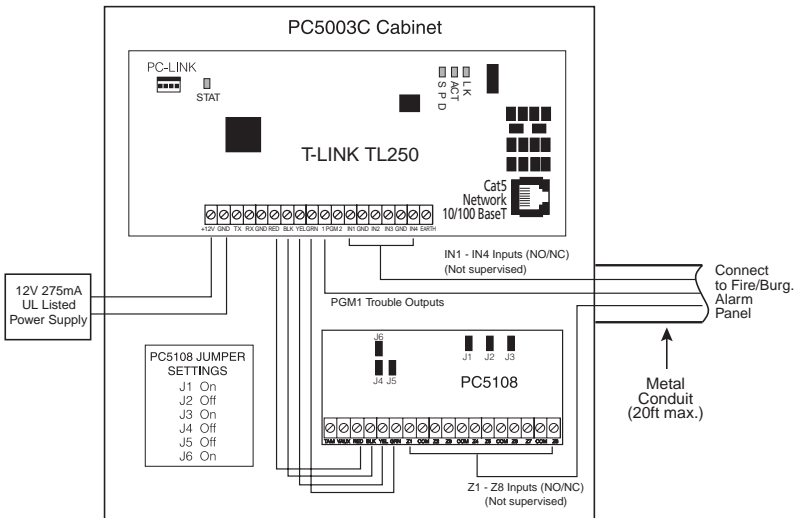
Section 5: Standard Installation (Mode 4)

5.1 Power864 and Maxsys Panel Setup and Installation

Refer to the *PC4020(CF) or PC5020(CF) Installation Manuals* for control panel installations. Mount the T-Link on the side wall of the PC4050C or PC4050CR cabinet. Refer to appendix C for Network Protection installation instructions.

Remove power 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.

5.2 Standard Connection with PC4020(CF)/PC5020(CF)

CAUTION: All circuits are supervised and power limited. Refer to section 5.4, 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.
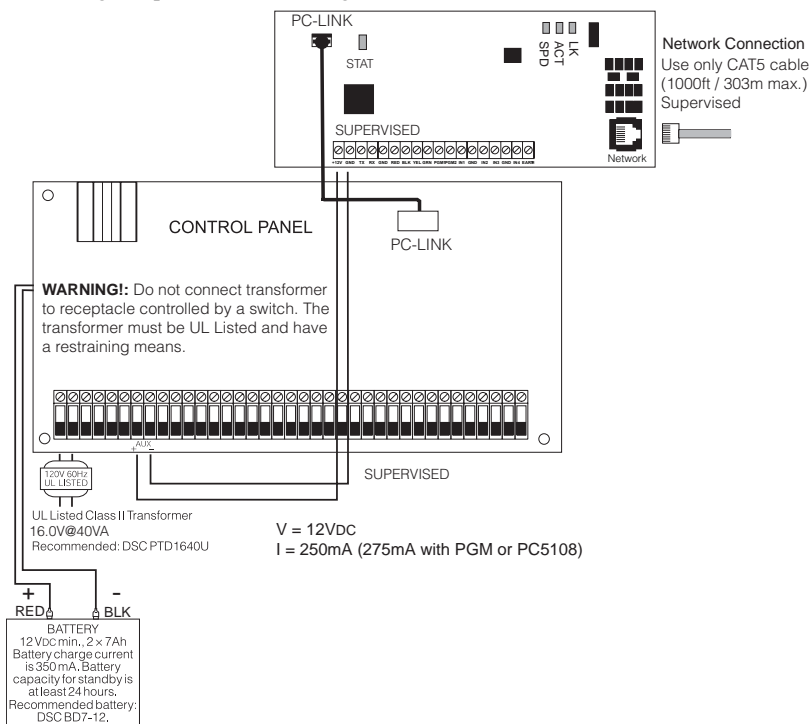
5.3   Wiring T-Link to a DSC Compatible Control Panel

• Secure the T-Link module to the side of the cabinet using the supplied standoffs.

• With AC power 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 will not 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. 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.*

5.4   Battery and AC Power Lead Routing for UL Listed Commercial Fire Systems
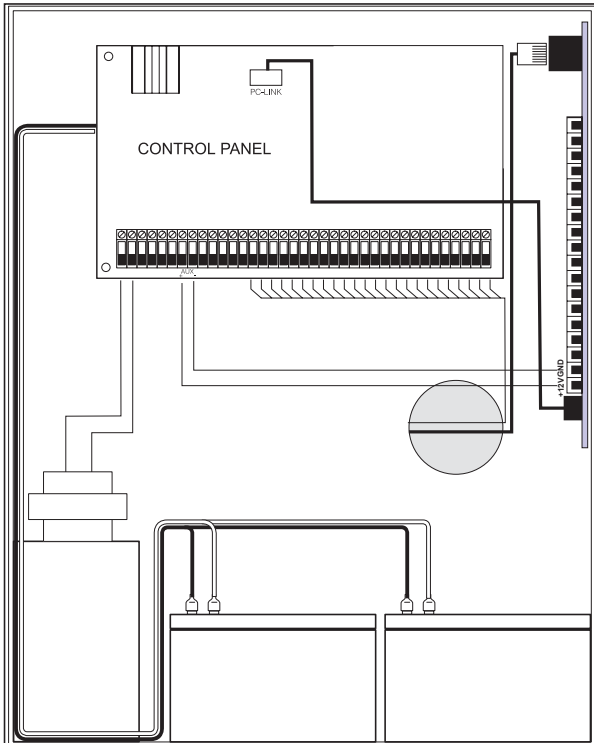
INSTALL BATTERY AND AC WIRING AS SHOWN ABOVE
IMPORTANT: A minimum ¼" (7mm) separation must be maintained at all points between battery/primary AC wiring and all other wiring and connections.

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

Section 6: DVACS Installation (Mode 5)

## 6.1   DVACS Panel Installation.

Remove power from the control panel before wiring connections to the T-Link TL250 module. Connect the 12VDC and GND terminals to the panel auxiliary power output. Connect the DVACS cable from the T-Link TL250 Adaptor on the PC-Link header to the DVACS connector on the control panel. Connect the e-ground to a proper earth-ground connection.

In a typical DVACS Installation, a DVACS panel is connected to an F1/F2 subset that communicates the alarm information to the central station comprising an SG MRL2 receiver with an SG DVL2A module installed.
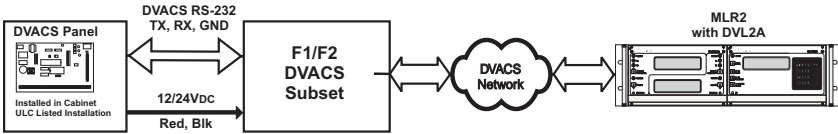
To send DVACS Alarm information over the internet, the T-Link TL250 performs the equivalent functions of the F1/F2 subset and the polling function of the SG DVL2A. DVACS alarm information is sent to the T-Link TL250 by connecting the existing RJ-45 terminated cable to the PC-Link Header on the TL250 module with an RJ-45 to PC-Link adaptor. The T-Link transmits DVACS alarm information in the DVACS protocol and T-Link Alarm information in the SIA protocol over the internet to a System III Receiver with SG-DRL3-IP line card installed.

Typical T-Link TL250/DVACS Installation
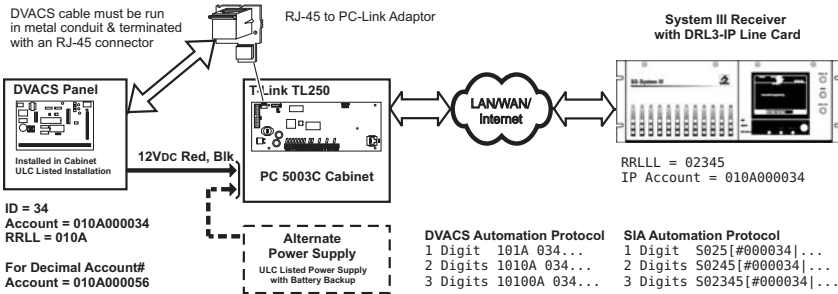
6.2   DVACS Events

DVACS events generated on DVACS panels connected through the T-Link TL250 follow the same protocols used on the SG-DVL2A module.

DVACS Alarms Examples

Example 1 (DVACS with receiver set as 1 digit line number)

Printer:

```
01 Nov 2004-11:38:22-01/02-SG -01-1-001--Burgl Alm Zn#02
```

Computer:

```
1011 001 A 02
```

Example 2 (DVACS with receiver set as 3 digits line number)

Printer:

```
01/02-SG -01-001-014--Burgl Alm Zn#13
```

Computer:

```
101001 014 A 13
```

SIA

DVACS Alarms Examples

Example 1 (DVACS with receiver set as 1 digit line number)

Printer:

```
01 Nov 2004-13:50:51-01/02-SG -01-1-0456--Fire Alm Zn999
```

Computer:

```
3011 0456FA 999
```

Example 2 (DVACS with receiver set as 3 digits line number)

Printer:

```
01 Nov 2004-13:51:03-01/02-SG -01-001-0456--Medical Alm Zn001
```

Computer:

```
3011 0456MA 001
```

Additional Events:

If the T-Link TL250 transmitter does not receive polls (response) from the panel, the T-Link will generate the events previously generated by the SG-DVL2A for DVACS panel and restoral.

SIA

Printer:

```
01 Nov 2004-13:50:51-01/02-SG -01-1-001--Account Absent
```

Computer:

```
3011 0001YC 000
```

Printer:

```
01 Nov 2004-13:50:51-01/02-SG -01-1-001--Account Present
```

Computer:

```
3011 0001YK 000
```

Standard

Printer:

```
01 Nov 2004-13:50:51-01/02-SG -01-1-001--IDcde IncResp
```

Computer:

```
1011 001 A 0A
```

Printer:

```
01 Nov 2004-13:50:51-01/02-SG -01-1-001--IDcde Restore
```

Computer:

```
1011 001 R 0A
```

NOTE: The SG-DRL3-IP will use 10-digit account identifications in it's IP table for DVACS transmitters. The first four digits represents the receiver and line number originally used on the SG-DVL2A and are programmed as the first four digits of the T-Link account (refer to appendix F of SG-DRL3-IP Installation Manual).

NOTE:If the automation protocol in the form of 1RRL, 3RRL is required when using the DRL3-IP in the DVACS configuration, set DRL3-IP Option [11] =1 and CPM3 Options [10] & [11] = 03

Section 7: TL300 Telephone Simulation

7.1   TL300 Panel Installation.
- Secure the T-Link module to the side of the cabinet of the control panel or install the T-Link TL300 in a DSC enclosure (model PC5003C). Refer to Appendix B: T-Link TL300 Compatibility Chart for a list of panels supported
- With AC power and battery disconnected removed from the control panel, connect the T-L300 to the RJ31 phone jack from the panel to the RJ31 connector on the T-Link.
- Wire the panel's 12VDC and GND terminals of T-Link or Power unit with a 12VDC 225 mA UL Listed Power supply.
- Wire the panel's Tip and Ring terminals to the T1 and R1 terminals of T-Link TL300.
- 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.
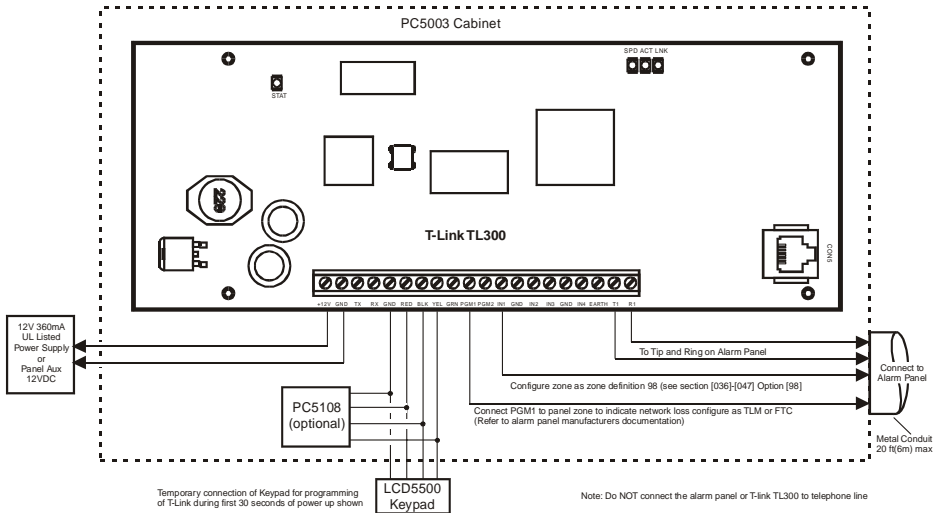
7.2   T-Link TL300 Operation.
Communication events between the panel, T-Link and the Central Station receiver are as follows:
- When an alarm triggers, the panel goes off-hook
- The T-Link module sends a dial tone to the panel
- The Panel dials the telephone number of the central station
- The T-Link detects the DTMF dialing and stops sending the dial tone.
- The T-Link sends a request to the Receiver.
- The Receiver responds with the command to the T-Link to generate the corresponding handshake.
- After receiving the handshake, the Panel transmits the alarm message in DTMF Contact ID format
- The T-Link decodes and transforms DTMF digits into an IP packet and sends it to the Receiver over IP.
- The Receiver acknowledges alarm and sends command to the T-Link to generate a corresponding kiss-off signal.
- After the T-Link generates kiss-off, the Panel goes on-hook if no more alarms need to be sent.

Section 8: T-Link Operation

8.1   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 service personnel are on-site.

8.2   Programming

The T-Link TL250/TL300 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 255.255.0.0 on port 3064.

8.3   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. Dynamic addressing (DHCP) can also 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.

8.4   Port Usage Table

NOTE: 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/ TL300	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	

8.5 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 reestablished 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.

NOTE: Receiver 2 is not supported for DVACS installations.

8.6 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 turn off when the network is absent.

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	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, 5020 or DVACS 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 '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
Receiver Version Mismatch	14	Indicates that the current Receiver software version requires updating. The present version may not support some alarms. **Note:**This applies to software versions v1.20 and higher

8.7 Testing & Troubleshooting

The T-Link TL250/TL300 and the System III Receiver can be connected directly with 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.

Upon T-Link 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.

The **Activity** and **Link LED**'s 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). Refer to the Status Indicator table above for details.

Section 9: Programming Guide

The following information is required Before programming the T-Link TL250/TL300 modules.

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 that 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.*

Important!: If a telephone line is used 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 programming T-Link TL250 to transmit first for faster 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 (30-45 seconds). This also applies when using the phone line for backup only.

9.1   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:

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; determine if this is required with the network administrator.

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	**CCCC = Receiver 2**
CBBB = Receiver 1	**CDDD = Receiver 3**

If the panel sends events to Receiver 0, 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.

9.2 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; verify with the network administrator if this is required.

9.3 T-Link DVACS Programming

Obtain the following information from the station monitoring the DVACS alarm panel:

1. The SG-DVL2A Receiver number and line number that the DVACS panel is connected to.
2. The DVACS panel ID (Account Number).
3. The programmed value of the SG-DVL2A extended format (option 07) for step 2 below.

Step 1: Program the Account Number of the DVACS control panel in the DVACS account option of the T-Link (option 067). The T-link will use this number to supervise the control panel and poll for DVACS signals from the panel.

NOTE: Alarms generated by the DVACS panel will be sent using the T-Link account.

Step 2: Program the T-Link DVACS extended option 068 so that it is identical to the SG-DVL2A extended option 07.

Step 3: Program the T-Link Account (option 003). To use the DVACS account number for alarm reporting, program the T-Link account option with this value.

When an alarm is sent from the DVACS control panel to the central station, the account number is expanded to a 10-digit value. The first four digits emulate the line number and receiver number on the MLR2/DVL2A. These four digits overwrite the SG-DRL3-IP receiver and line number before being sent to the printer and computer. This allows existing DVACS accounts to be sent to the automation software without alteration and account duplication on the same SG DRL3-IP line card using a different line and/or receiver number.

NOTE: If a new account is created, the first four digits must be programmed as '0000'.

9.4   T-Link TL300 Programming

Step 1: Program the static IP address for the T-Link TL300 module in section [001].

Program 000.000.000.000 for DHCP

Step 2: Program the subnet mask for T-Link TL300 in section [002] if required.

This option will be ignored if the unit is set for DHCP (Section [001])

Step 3: Program the static IP address of the receiver (DRL3-IP line card) in section [007].

Step 4: If the receiver (DRL3 -IP line card) is on a different network segment than the T-Link TL300 module, Program the gateway address associated with the T-Link TL300 in section [008].

NOTE: This step is optional. Verify with the Network Administrator if this step is required.

Step 5: If a specific dial tone is required for the panel connected to T-LinK TL-300 T1/R1, refer to section [071].

Section 10: Programming Descriptions (Advanced)

[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: 255.255.0.0

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: 0000FFFFFF

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: Account codes 0000FFFFFF, FFFFFFFFFF and 0000000000 are not valid accounts. Refer to section 5.3 T-Link DVACS Programming.

[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 (default 5555) is required 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 must 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 E-mail 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.

If Contact ID messages are received from the panel, the e-mail will be sent as:

From: T-Link 123456

To: recipient@address.com

Subject: T-Link v1.2.xx; 123456 Event Report

Message: 6789s1s100s01ss001sMedical

NOTE:The text length will have a maximum number of characters that will be equal to the longest Contact ID message. A space will be inserted for every "s" above.

[028] 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 this option is programmed with any string, the value in the 'FROM' field will be programmed in this 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 with T-Link Console software.

[031] E-mail 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 with T-Link Console software.

[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 With T-Link Console software.

[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

Must 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.

    PGM1-The PGM1 output is dedicated for T-Link TL250 trouble indications. Program this option as '01' for Modes 2 & 3,.

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.
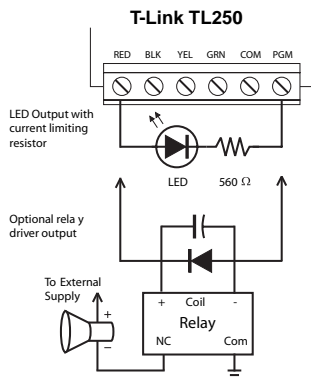
    PGM2-The PGM2 output is dedicated as an input follower that is triggered on any input alarm (including Bell Follower which generates Burglary and Fire Alarms) except for key-switch zones. The PGM2 output will only turn off when ALL violated zones are restored.

NOTE: PGM2 is always enabled and follows all zones. It is the users option to connect devices to the PGM.

[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.

[98] 24-hr. Panel Absent.

When this input is violated, the T-Link immediately communicates to the central station

SIA Reporting Code: ET001/ER001.

[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. Refer to options [062] through [065].

Mode 1 - Bell Follower Operation
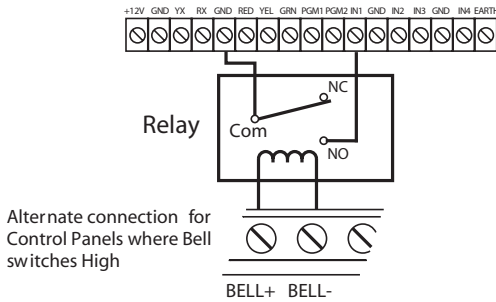
[048] Input 1 Configuration

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 hard coded input number.

If anything between 01 and 99 is programmed, the hard coded 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

Default: 64

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

Default: 03

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

Default: 02

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

[067] DVACS Account Number

Default: 00

The DVACS Account Number. The T-Link will use this number to receive DVACS signals from the control panel and to supervise the panel.

[068] DVACS Extended

Default: 01

The SG-DV1660LC software versions 3.00 and higher support the group arm/disarm option. If a value other than '00' is programmed here, the T-Link TL250 will poll the subscriber's control unit repeatedly to get the transmitter group number arm/disarm status change and the user number. This information is combined then sent to the receiver. This allows the automation software to keep track of partition arm/disarm status. Program '01' to enable or '00' to disable this option.

Example, Option Enabled '01'

Printer:

```
01 Nov 2004-11:38:22-01/02-SG -01-1-001--012- Grp 1 Arming!B4
01 Nov 2004-11:38:22-01/02-SG -01-1-001--012- Grp 2 Arming!B5
01 Nov 2004-11:38:22-01/02-SG -01-1-001--012- Close User# 01
```

Computer:

```
1011sssssss012sC1s01
1011sssssss012sC2s01
```

Computer message combining for DVACS SIA protocol

```
3RRLssssss0AAAOGs002 (partition(OG/CG)
```

```
3RRLssssss0AAAOPs001 (user number)
```

Computer message combining When DVACS extended option enabled

```
SRRL[#AAAA|Nri2/OP001][14]
```

NOTE:This will support 0-F group numbers maximum.

[069] TL300 Contact ID Kiss-off Duration

Default: 08

Some control panels may require a different kiss-off duration than the default of 800ms. Program this option for the duration of the Contact ID kiss off provided to the panel. Each unit has increments of 100 ms in hex, from 100 ms to a maximum of 8.1 seconds.

> For example: 08 = 800 ms
>
> 0A = 1000 ms (1 second)

NOTE:Kiss-off durations greater than 1.5 seconds may not be compatible with some alarm panel. This may be required for special applications. Kiss-off durations higher than 8.1 seconds will not be accurate and may not match the duration programmed.

[070] TL300 Contact ID Handshake Selection

Default: 2D

1400Hz or Dual tone Handshake can be selected.

Enter "2D" for Dual Tone or Enter "14" for 1400Hz

[071] TL300 Dialtone Selection

Default: 00

Enter the 2-digit code corresponding to country indicated in the table below.

Code	Country	Code	Country
00	United States/ Canada	08	Norway
01	The Netherlands	09	Sweden
02	United Kingdom	0A	Switzerland
03	South Korea	0B	Australia
04	Taiwan	0C	France
05	Italy	0D	Belgium
06	Brazil	0E	Future Use
07	Germany	0F	Future Use

[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 module will respond with the current IP address of the T-Link and display it on the keypad for the user.

Section 11: Programming Worksheets

Sect. Description	Default Value
001 T-Link IP Address	192.168.0.99
|⎵⎵⎵⎵| |⎵⎵⎵⎵| |⎵⎵⎵⎵| |⎵⎵⎵⎵|	
002 T-Link Subnet Mask	255.255.0.0
|⎵⎵⎵⎵| |⎵⎵⎵⎵| |⎵⎵⎵⎵| |⎵⎵⎵⎵|	
003 T-Link Account Code	0000FFFFFF
|⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵|	
004 Receiver Encryption Password	0000000000000000
|⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵|	
005 Receiver Encryption Password	0000000000000000
|⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵⎵|	
006 Installer Code	5555
|⎵⎵⎵⎵|	
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
|⎵⎵⎵⎵|	
020 TFTP port	69
|⎵⎵|	
021 DLS Port	3062

Sect.	Description	Default Value
	|__|__|__|__|__|	
022	SA Port	3063
	|__|__|__|__|__|	
023	Supervision Enable (UL/ULC option must be set to 1)	00
	|__|__|	
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	E-mail Account	Null
	|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|	
032	E-mail 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)
	|__|__|	
041	Digital Input 06 Definition	00 (Disabled)
	|__|__|	
042	Digital Input 07 Definition	00 (Disabled)
	|__|__|	
043	Digital Input 08 Definition	00 (Disabled)

Sect.	Description	Default Value
	└──┴──┘	
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
	└──┴──┘	
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

Sect. Description	Default Value
⌊___⌋___⌋	
065 Fire Pulse Count	0x03
⌊___⌋___⌋	
066 SIA ACK Time	0x02
⌊___⌋___⌋	
067 DVACS Account	0x00
⌊___⌋___⌋	
068 DVACS Extended	01 (Disabled)
⌊___⌋___⌋	
069 Contact ID Kiss-off Duration	0x08
⌊___⌋___⌋	
070 Contact ID Handshake Selection	0x2D
⌊___⌋___⌋	
071 TL300 Dial Tone Generation Selection	0x00
⌊___⌋___⌋	
901 Current T-Link IP Address	

⌊___⌋___⌋___⌋ ⌊___⌋___⌋___⌋ ⌊___⌋___⌋___⌋ ⌊___⌋___⌋___⌋

Glossary

Console

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

DHCP

Dynamic Host Configuration Protocol, 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.

DVACS®

Digital Voice Access Control System This monitoring method requires a dedicated leased line from Bell Canada connected between the alarm system and the monitoring station. It is supervised so that if the line is cut an alarm will occur. This system is only available in Canada and meets ULC certification requirements. DVACS is a registered trademark of Electro Arts Ltd. Scarborough Ontario Canada

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 *Institute of Electrical and Electronics Engineers*, 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 *Internet Protocol*, 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 *Media Access Control* 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

Multipurpose Internet Mail Extensions, 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 *Transport Control Protocol*, 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 TL250 Compatibility Chart

MAXSYS PC4020	• Software V3.31 or higher • Hardware Rev 04B
Power864 PC5020	• Software V3.2 or higher • Hardware Rev 03
DVACS Panels	• DV1660 LCD V5.03 • DV1660 LED V3.01 • DV4420 V1.11 • DVCOM • DV4T • PC5400DV • PC4400DV • PC4401DV
T-Link TL250/300	• 10/100 BaseT • TCP/IP communication module • Static or DHCP IP configurable • Additional zone inputs using PC5108 • Program locally using PowerSeries keypad.
SG-DRL3-IP V1.20 *	• Supports 1024 accounts, maximum 512 accounts can be supervised • Static IP required for DRL3-IP
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
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
T-Link Console V1.20	• Required • Free download from dsc.com with a valid password
NOTE: The DLS software can only be used with UL Listed installations when service personnel are on-site.	

Appendix B: T-Link TL300 Compatibility Chart

DSC	• PC580 • PC1555 • PC4010 • PC6010 • PC5010 • SN4030
DMP	• XR-10 • XR-20 • XR-200 • XR-500
FBI	• 4600
GE	• Simon • Concord • Concord Ultra
Honeywell	• Vista 20P
Napco	• 2600
Paradox	• Digiplex 848
NOTE: In general, the T-LINK TL300 will be compatible with any panel with a DTMF tone and silence duration of greater than 40 ms, and with a signal levels within FCC accepted levels. (typical -9db)	

Appendix C: TL250/TL300 T-Link Events

T-Link events sent to the central station.

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: Contact ID Reporting Codes

Contact ID Format:

CCCC Q EEE GG ZZZ

CCCC = customer (subscriber account number)
Q = event qualifier, E = new Event, R = Restore
EEE = event code
ZZZ = zone ID number reporting the alarm (001-099), or user number for open/close reports.

> **Note:** System status messages (e.g.,AC Loss, Low Battery etc.) contain zeros in the ZZZ location

Subscriber ID #	Event Qualifier Event or Restore	Event Coded	Partition #	Zone or User #
XXXX	**E** or **R**	000	00	C000 or U000

MEDICAL:
100	Medical	Emerg-PersonalEmergency-#
101	Pendant Transmitter	Emerg-Personal Emergency-#
102	Fail to report in	Emerg-Fail to check in-#

FIRE ALARMS:
110	FIRE	Fire-Fire Alarm-#
111	SMOKE w/VERIFICATION	Fire-Fire Alarm-#
112	Combustion	Fire-Combustion-#
113	WATERFLOW	Fire-Water Flow -#
114	Heat	Fire-Heat Sensor-#
115	Pull Station	Fire-Pull Station-#
116	Duct	Fire-Duct Sensor-#
117	Flame	Fire-Flame Sensor-#
118	Near Alarm	Fire-Near Alarm -#

PANIC ALARMS:
120	Panic Alarm	Panic-Panic-#
121	DURESS	Panic-Duress- User 000, or duress zone number on low end panels
122	SILENT	Panic-Silent Panic-#
123	AUDIBLE	Panic-Audible Panic-#
124	Duress-Access	Granted Panic-Duress Access Grant-#
125	Duress-Egress	Granted Panic-Duress Egress Grant-#

BURGLAR ALARMS:
130	Burglary	Burg-Burglary-#
131	PERIMETER	Burg-Perimeter-#
132	INTERIOR	Burg-Interior-#
133	24 HR BURG (AUX)	Burg-24 Hour-#
134	ENTRY/EXIT	Burg-Entry/Exit-#
135	DAY/NIGHT	Burg-Day/Night-#
136	Outdoor	Burg-Outdoor-#
137	TAMPER	Burg-Tamper-#
138	Near Alarm	Burg-Near Alarm-#
139	Intrusion Verifier	Burg-Intrusion Verifier-#

GENERAL ALARMS:
140	General Alarm	Alarm-General Alarm-#
141	Polling Loop Open	Alarm-Polling Loop Open
142	POLLING LOOP SHORT (AL)	Alarm-Polling Loop Short
143	EXPANSION MOD FAILURE	Alarm-Exp. Module Tamper-#

144	Sensor Tamper	Alarm-Sensor Tamper-#
145	Expansion Module Tamper	Alarm-Exp. Module Tamper-#
146	SILENT BURG	Burg-Silent Burglary-#
147	Sensor Supervision	Trouble – Sensor Super. -#

24 HOUR NON-BURGLARY:

150	24 HOUR (AUXILIARY)	Alarm-24 Hr. Non-Burg-#
151	Gas Detected	Alarm-Gas Detected-#
152	Refrigeration	Alarm-Refrigeration-#
153	Loss of Heat	Alarm-Heating System-#
154	Water Leakage	Alarm-Water Leakage-#
155	Foil Break	Trouble-Foil Break-#
156	Day Trouble	Trouble-Day Zone-#
157	Low Bottled Gas Level	Alarm-Low Gas Level-#
158	High Temp	Alarm-High Temperature-#
159	Low Temp	Alarm-Low Temperature-#
161	Loss of Air Flow	Alarm-Air Flow-#
162	Carbon Monoxide Detected	Alarm-Carbon Monoxide-#
163	Tank Level	Trouble-Tank Level-#

FIRE SUPERVISORY:

200	FIRE SUPERVISORY	Super.-Fire Supervisory-#
201	Low Water Pressure	Super-Low Water Pressure-#
202	Low CO2	Super.-Low CO2-#
203	Gate Valve Sensor	Super.-Gate Valve-#
204	Low Water Level	Super.-Low Water Level-#
205	Pump Activated	Super.-Pump Activation-#
206	Pump Failure	Super.-Pump Failure-#

SYSTEM TROUBLES:

300	System Trouble	Trouble-System Trouble
301	AC LOSS	Trouble-AC Power
302	LOW SYSTEM BATT	Trouble-Low Battery (AC is lost, battery is getting low)
326	Notification Appliance Ckt. # 3	Trouble-Notification Appl. Ckt#3
327	Notification Appliance Ckt. # 4	Trouble-Notification Appl. Ckt#4

SYSTEM PERIPHERAL TROUBLES:

R330	System Peripheral (E355)	Trouble-Sys. Peripheral-# From LRR, ECP data connection to panel.
331	Polling Loop Open	Trouble-Polling Loop Open
332	POLLING LOOP SHORT	Trouble-Polling Loop Short
333	Exp. Module Failure (353)	Trouble-Exp. Module Fail-# ECP Path problem between panel to LRR, etc (new)
334	Repeater Failure	Trouble-Repeater Failure-#
335	Local Printer Paper Out	Trouble-Printer Paper Out
336	Local Printer Failure	Trouble-Local Printer
337	EXP. MOD. DC LOSS	Trouble-Exp. Mod. DC Loss-#
338	EXP. MOD. LOW BAT	Trouble-Exp. Mod. Low Batt-#
339	EXP. MOD. RESET	Trouble-Exp. Mod. Reset-#
341	EXP. MOD. TAMPER	Trouble-Exp. Mod. Tamper-# (5881ENHC)
342	Exp. Module AC Loss	Trouble-Exp. Module AC Loss-#
343	Exp. Module Self Test Fail	Trouble-Exp. Self-Test Fail-#
344	RF Rcvr Jam Detect #	Trouble-RF Rcvr Jam Detect-#

COMMUNICATION TROUBLES:

350	Communication	Trouble-Communication Failure
351	TELCO 1 FAULT	Trouble-Phone line # 1 Comes in as zone 1 on a V20P panel
352	TELCO 2 FAULT	Trouble-Phone Line # 2
353	LR Radion Xmitter Fault (333)	Trouble-Radio Transmitter – Comm Path problem between panel and lrr (0ld)
354	FAILURE TO COMMUNICATE	Trouble-Fail to Communicate
E355	Loss of Radio Super. (R330)	Trouble-Radio Supervision – From LRR - ECP data connection to panel
356	Loss of Central Polling	Trouble-Central Radion Polling
357	LRR XMTR. VSWR	Trouble-Radio Xmitter. VSWR-#

PROTECTION LOOP:

370	Protection Loop	Trouble-Protection Loop-# (zone type 19)

Note: *Uplink cell backup devices send zone 99 for a low battery and a zone 97 for communication failure (no response from poll). These will report as contact ID E370 (protection loop). let me clarify this: these are signals GENERATED by the uplink to indicate STATUS of the uplink. The central station will assume that they were generated by the panel. Additional codes that may be sent would be for zones 81-86 which correspond to hardwire inputs 1-6. The contact ID message for these is selected by uplink when it is programmed. So, next time someone reports an unusual zone 97 or 99 being reported to their Central Station, Uplink may be the culprit. Uplink's number is 1-888-987- 5465 if you need it.*

371	Protection Loop Open	Trouble-Prot. Loop Open-#
372	Protection Loop Short	Trouble-Prot. Loop Short-#
373	FIRE TROUBLE	Trouble-Fire Loop-# (Supervision Loss,base tamper, Supervisory open)
374	EXIT ERROR (BY USER)	Alarm-Exit Error-#
375	Panic Zone Trouble	Trouble-PA Trouble-#
376	Hold-Up Zone Trouble	Trouble-Hold-Up Trouble-#
377	Swinger Trouble	Trouble – Swinger Trouble-#
378	Cross-zone Trouble	Trouble – Cross Zone Trouble - # (restore not applicable)

SENSOR:

380	SENSOR TRBL - GLOBAL	Trouble-Sensor Trouble-#
381	LOSS OF SUPERVISION	Trouble-RF Sensor Super.-#
382	LOSS OF SUPRVSN	Trouble-RPM Sensor Super.-#
383	SENSOR TAMPER	Trouble-Sensor Tamper-#
384	RF LOW BATTERY	Trouble-RF Sensor Battery-#
385	SMOKE HI SENS.	Trouble-Smoke Hi Sens.-#
386	SMOKE LO SENS.	Trouble-Smoke Lo Sens.-#
-387	INTRUSION HI SENS.	Trouble-Intrusion Hi Sens.-#
-388	INTRUSION LO SENS.	Trouble-Intrusion Lo Sens.-# - These codes are similar to those used for smart smoke detectors. The idea is to report a problem developing in the detector's operation.
389	DET. SELF TEST FAIL	Trouble-Sensor Test Fail-#
391	Sensor Watch Failure	Trouble-Sensor Watch Fail-#
392	Drift Comp. Error	Trouble-Drift Comp. Error-# - Reported by Firelite panels. The panel is not able to adjust its thresholds to balance out drift in the normal operating point of a smoke detetctor.
393	Maintenance Alert	Trouble-Maintenance Alert-#

OPEN/CLOSE:

400	Open/Close	Opening/Closing E = Open, R = Close
401	OPEN/CLOSE BY USER	Opening-User # / Closing-User #
402	Group O/C	Closing-Group User #
403	AUTOMATIC OPEN/CLOSE	Opening-Automatic / Closing-Automatic
404	Late to O/C	Opening-Late / Closing-Late
405	Deferred O/C	Event & Restore Not Applicable
406	CANCEL (BY USER)	Opening-Cancel
407	REMOTE ARM/DISARM	Opening-Remote / Closing-Remote
408	QUICK ARM	Event Not Applicable for opening / Closing-Quick Arm
409	KEYSWITCH OPEN/CLOSE	Opening-Keyswitch / Closing-Keyswitch
435	Second Person Access	ACCESS – User #
436	Irregular Access	ACCESS – Irregular Access – User #
441	Armed Stay	Opening-Armed Stay / Closing-Armed Stay
442	Keyswitch Armed Stay	Opening-Keysw. Arm Stay / Opening-Keysw. Arm Stay
450	Exception O/C	Opening-Exception / Closing-Exception
451	Early O/C	Opening-Early / Closing-Early-User #
452	Late O/C	Opening-Late / Closing-Late-User #
453	Failed to Open	Trouble-Fail to open (Restore not applicable)
454	Failed to Close	Trouble-Fail to Close (Restore not applicable)
455	Auto-Arm Failed	Trouble-Auto Arm Failed (Restore not applicable)
456	Partial Arm	Closing-Partial arm-User #
457	Exit Error (User)	Closing-Exit Error-User #
458	User on Premises	Opening-User on Prem. – User #

459	Recent Close	Trouble-Recent Close – User # (Restore not applicable)
461	Wrong Code Entry	Access – Wrong Code entry (Restore not applicable)
462	Legal Code Entry	Access-Legal Code entry – user # (Restore not applicable)
463	Re-arm after Alarm	Status-Re Arm After Alarm-User # (restore not applicable)
464	Auto Arm Time Extended	Status-Auto Arm Time Ext. – User # (Restore not applicable)
465	Panic Alarm Reset	Status-PA Reset (Restore not applicable)
466	Service On/Off Premises	Access – Service **ON** Prem – User #
		Access – Service **OFF** Prem – User #

REMOTE ACCESS:

411	CALLBACK REQUESTED	Remote-Callback Requested (No Restore) Enabled with O/C reports
412	Success-Download/access	Remote-Successful Access (Restore Not Appllicable)
413	Unsuccessful Access	Remote-Unsuccessful Access (Restore Not Applicable)
414	System Shutdown	Remote-System Shutdown
415	Dialer Shutdown	Remote-Dialer Shutdown
416	Successful Upload	Remote-Successful Upload (Restore Not Applicable)

ACCESS CONTROL:

421	Access Denied	Access-Access Denied-User # (Restore Not Applicable)
422	Access Report by User	Access-Access Gained –User# (Restore Not Applicable)
423	Forced Access	Panic-Forced Access-#
424	Egress Denied	Access-Egress Denied (Restore Not Applicable)
425	Egress Granted	Access-Egress Granted-# (Restore Not Applicable)
426	Access Door Propped Open	Access-Door Propped Open-#
427	Access Point DSM Trouble	Access-ACS Point DSM Trbl.-#
428	Access Point RTE Trouble	Access-ACS Point RTE Trbl.-#
429	Access Program Mode Entry	Access-ACS Prog. Entry-User # (Restore Not Applicable)
430	Access Program Mode Exit	Access-ACS Prog. Exit-User # (Restore Not Applicable)
431	Access Threat Level Change	Access-ACS Threat Level Chg.
432	Access Relay/Trigger Fail	Access-ACS Relay/Trig. Fail-#
433	Access RTE Shunt	Access-ACS RTE Shunt-#
434	Access DSM Shunt	Access-ACS DSM Shunt-#

SYSTEM DISABLES:

| 501 | Access Reader Disable | Disable-Access Rdr. Disable-# |

SOUNDER/RELAY DISABLES:

520	Sounder/Relay Disable	Disable-Sounder/Relay-#
521	Bell 1 Disable	Disable-Bell/Siren # 1
522	Bell 2 Disable	Disable-Bell/Siren # 2
523	Alarm Relay Disable	Disable-Alarm Relay
524	Trouble Relay Disable	Disable-Trouble Relay
525	Reversing Relay Disable	Disable-Reversing Relay
526	Notification Appliance Ckt # 3	Disable-Notification Appl. Ckt#3
527	Notification Appliance Ckt # 4	Disable-Notification Appl. Ckt#4

SYSTEM PERIPHERAL DISABLES:

| 531 | Module Added | Super.-Module Added (Restore Not Applicable) |
| 532 | Module Removed | Super.-Module Removed (Restore Not Applicable) |

COMMUNICATION DISABLES:

551	Dialer Disabled	Disable-Dialer Disable
552	Radio Xmitter Disabled	Disable-Radio Disable
553	Remote Upload/Download	Disable-Rem. Up/download Disable

BYPASSES:

570	ZONE/SENSOR BYPASS	Bypass-Zone Bypass-#
571	Fire Bypass	Bypass-Fire Bypass-#
572	24 Hour Zone Bypass	Bypass-24 Hour Bypass-#
573	Burg. Bypass	Bypass-Burg. Bypass-#
574	Group Bypass	Bypass-Group Bypass-User #
575	SWINGER BYPASS	Bypass-Swinger Bypass-#
576	Access Zone Shunt	Access-ACS Zone Shunt-#
577	Access Point Bypass	Access-ACS Point Bypass-#
578	Zone Bypass	Bypass – Vault Bypass - #
579	Zone Bypass	Bypass – Vent Zone Bypass - #

TEST / MISC:

601	MANUAL TEST	Test-Manually Triggered (Restore Not Applicable)
602	PERIODIC TEST	Test-Periodic (Restore Not Applicable
603	Periodic RF Xmission	Test-Periodic Radio (Restore Not Applicable)
604	FIRE TEST	Test-Fire Walk Test-User #
605	Status Report To Follow	Test-Fire Walk Test-User #
606	LISTEN-IN TO FOLLOW	Listen-Listen-In Active (Restore Not Applicble)
607	WALK-TEST MODE	Test-Walk Test Mode-User #
608	System Trouble Present	Test-System Trouble Present (Restore Not Applicable)
609	VIDEO XMTR ACTIVE	Listen-Video Xmitter Active (Restore Not Applicable)
611	POINT TESTED OK	Test-Point Tested OK-# (Restore Not Applicable)
612	POINT NOT TESTED	Test-Point Not Tested-# (Restore Not Applicable)
613	Intrusion Zone Walk Tested	Test-TntrnZone Walk Test-# (Restore Not Applicable)
614	Fire Zone Walk Tested	Test-Fire Zone Walk Test-# (Restore Not Applicable)
615	Panic Zone Walk Tested	Test-PA Zone Walk Test (Restore Not Applicable)
616	Service Request	Trouble-Service Request

EVENT LOG:

621	EVENT LOG RESET	Trouble-Event Log Reset (Restore Not Applicable)
622	EVENT LOG 50% FULL	Trouble-Event Log 50% Full (Restore Not Applicable)
623	EVENT LOG 90% FULL	Trouble-Event Log 90% Full (Restore Not Applicable)
624	EVENT LOG OVERFLOW	Trouble-Event Log Overflow (Restore Not Applicable)
625	TIME/DATE RESET	Trouble-Time/Date Reset-User # (Restore Not Applicable)
626	TIME/DATE INACCURATE	Trouble-Time/Date Invalid (clock not stamping to log correctly)
627	PROGRAM MODE ENTRY	Trouble-Program Mode Entry (Restore Not Applicable)
628	PROGRAM MODE EXIT	Trouble-Program Mode Exit (Restore Not Applicable

SCHEDULING:

630	Schedule Change	Trouble-Schedule Changed (Restore Not Applicable)
631	Exception Sched. Change	Trouble-Esc. Sched. Changed (Restore Not Applicable)
632	Access Schedule Change	Trouble-Access Sched. Changed (Restore Not Applicable)

PERSONNEL MONITORING:

641	Senior Watch Trouble	Trouble-Senior Watch Trouble – This code is also refered to as 'up and about'. It means that a person has not moved about their home for a preset period of time.
642	Latch-key Supervision	Status-Latch-key Super-User # (Restore Not Applicable) Used to report when a certain user has returned home and disarmed the alarm.

SPECIAL CODES:

651		Code sent to Identify the control panel as an ADT Authorized Dealer.
750-789		These codes are used by Protection One and can be assigned any unique non-standard Event code, which Pro 1 will be tracking. Also can be used on custom zone types.

Miscellaneous:

654	System Inactivity	Trouble – System Inactivity
900	Download Abort	Remote – Download Abort (Restore not applicable)
901	Download Start/End	Remote – Download Start - #
		Remote – Download End - #
902	Download Interrupted	Remote – Download Interrupt - #
910	Auto-Close with Bypass	Closing – Auto Close – Bypass - #
911	Bypass Closing	Closing – Bypass Closing - #

Other:

999	1 and 1/3 DAY NO READ LOG	EVENT LOG ONLY, No report to CS. V20/lynx series or may occur in Vista-50 family after a download is done where the account has been transferred from one panel type to another. (i.e. from and XMP to a 50P, etc).

Appendix E: Network Protection

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

To Network

Ferrite
DSC PN 10000089

To T-Link
Network
Connector
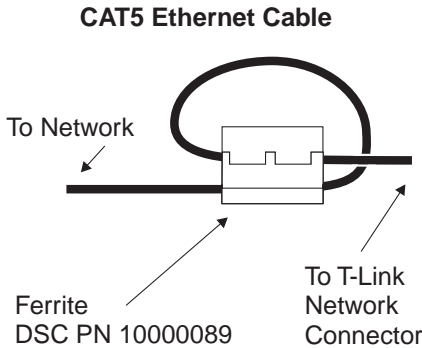
NOTE:

I**nstall 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).

INSTALLATION of RJ-45 to RJ-45 Mounting Plate (CE Installations Only)

Drilling Template

31401 REVA

CAT 6
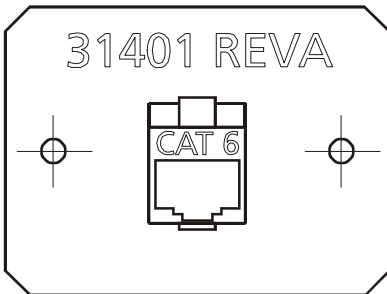
Installation:

1. Remove the knockout located on the top right hand side of the cabinet.
2. Drill 2 holes in cabinet location using the drill template and 2.5mm (3/16") drill bit.
3. Secure the mounting plate externally to the cabinet using the #6 Type F, self-tapping screws provided.
4. Connect RJ-45 cables observing the "Important" notice indicated above.
5. Verify operation.

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.

DSC®

29034631R005