T-Link

Network Alarm Communicator

Installation Manual

v 1.0

Toronto, Canada • **www.dsc.com**
Tech Support (Canada & US) 1-800-387-3630
Printed in Canada 29001007 R002

Direct all comments concerning this publication to **pubs@dscltd.com**

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 emergency situation.

LIMITED WARRANTY

Digital Security Controls Ltd. 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 Ltd. 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 Ltd. 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 Ltd. 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 Ltd. must first obtain an authorization number. Digital Security Controls Ltd. 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 Ltd. 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 Ltd.);
- 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 Ltd.'s 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 Ltd. 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 Ltd. Digital Security Controls Ltd. 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.

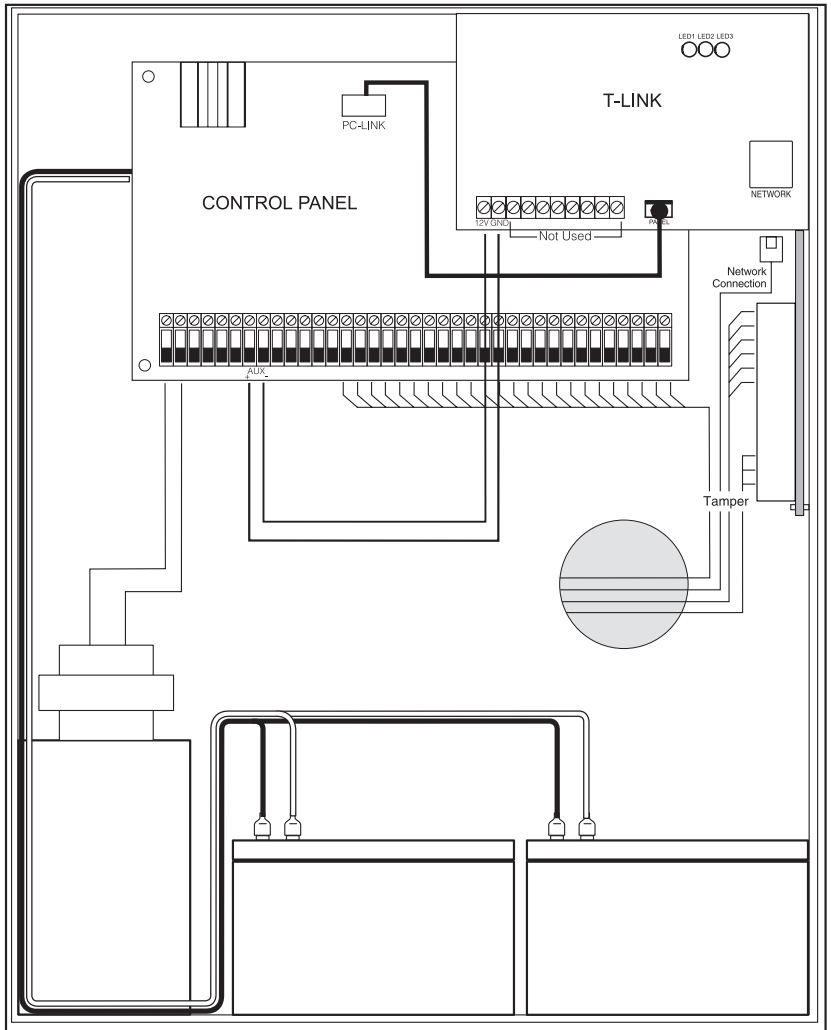
WARNING: Digital Security Controls Ltd. recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.

Out of Warranty Repairs

Digital Security Controls Ltd. 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 Ltd. must first obtain an authorization number. Digital Security Controls Ltd. will not accept any shipment whatsoever for which prior authorization has not been obtained.

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

5.3 Battery Lead and AC Power Lead Routing for UL Listed Commercial Fire Systems



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

T-Link board could be installed on a mounting bracket or on the side of the cabinet. Please refer to mounting instructions in this manual.

T-Link Compatibility Chart

FCC Compliance Statement

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

T-Link Compatibility Chart

Compatible DSC Control Panels	
Maxsys PC4020	• Software V3.31 or higher • Hardware Rev 04B
Power864 PC5020	• Software V3.2 or higher • Hardware Rev 03
TCP/IP Communicator	
T-Link	• 10baseT TCP/IP communication module • Static IP required per module
TCP/IP Communication Routing / Receiver	
Reporter IP V2.0	• Required for T-Link communications and DLS • Supports 255 T-Link accounts, one DLS-3 and one DLS-3SA at the same time. • **Not for UL Listed installations** • Static IP required for computer
DRL-IP V1.0 *	• Required for T-Link communications and DLS • Supports 255 supervised T-Link accounts, one DLS-3 and one DLS-3SA at the same time. • Static IP required per DRL-IP
Downloading Software	
DLS-3 V1.3	• 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 V1.3 service pack	• Free download from dsc.com with a valid password
System Administration Software	
DLS-3 SA V1.3	• Required • Kit with modem or PC4401 from distributor
DLS-3 SA V1.3 Service Pack 1 for Maxsys V3.31 support	• Required • Included in the kit or free download from dscsec.com/dls3drivers.htm
DLS-3 SA V1.3 Service Pack 2 for Power864 v3.2 support	• Required • Included in the kit or free download from dscsec.com/dls3drivers.htm

***NOTE:**
The DLS software could be used with UL Listed installations only when a service personnel is on the site.

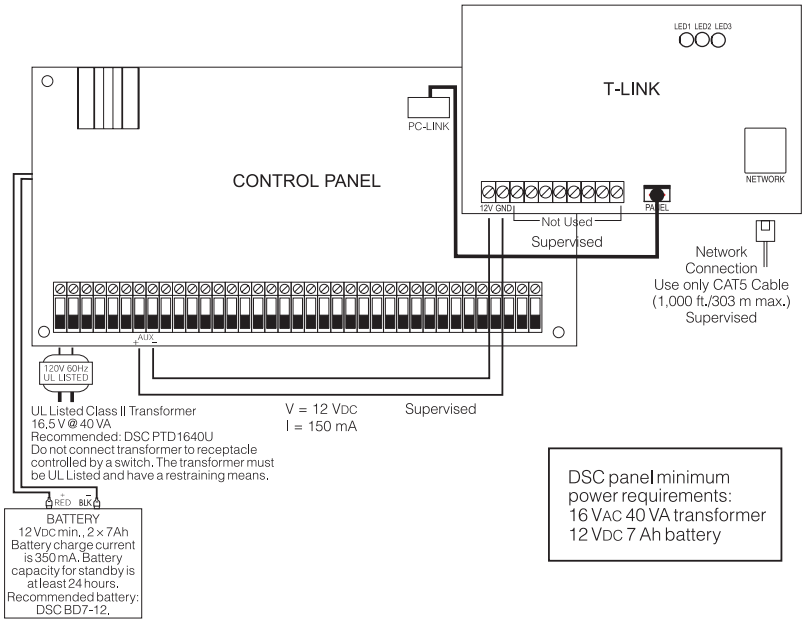
5.2 Standard Connection with PC4020(CF)/PC5020(CF)

WARNING!

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

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

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

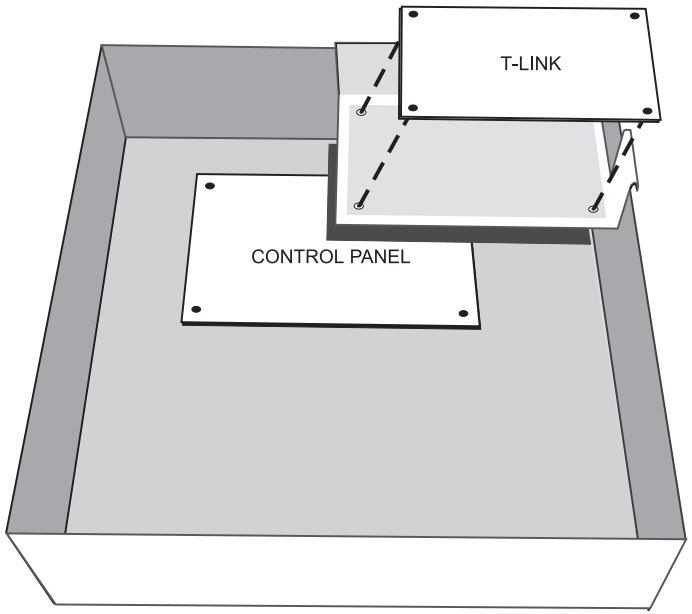


Wiring T-Link to a DSC Compatible Control Panel

- Mount the T-Link using bracket or on the side of the cabinet.
- Secure the T-Link module to the cabinet using the supplied standoffs.
- With both AC and battery disconnected removed from the DSC control panel, wire the T-Link to the panel using 4 wires from the PC-Link of the panel to the "PANEL" connector on the T-Link.
- Wire the panel's AUX + and - to 12V 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.

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

5.1 Mounting T-Link Using HMB-1 Bracket



Mounting Instructions

Step 1: Mount the Control panel cabinet and PCB as per the panel's installation instructions

Step 2: Insert the four nylon standoffs from the bottom of the HMB-1 bracket

Step 3: Push the HMB-1 hangers onto the top right corner of the panel cabinet

Step 4: Align the T-link mounting holes with the standoffs on the HMB-1 and snap into place

Step 5: Wire the T-Link module to the control panel (refer to pages 13 and 14 for wiring instructions)

Ethernet

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

IEEE

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

Intranet

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

IP

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

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

IP Address

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

LAN

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

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

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 what subnet an **IP address** belongs to.

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

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.

[020] System Status

If option [2] is on, the T-Link module will supervise communication with the receiver. If option [2] is OFF, no trouble will be generated if communication is lost with the receiver. (Recommended OFF)

If option [3] is on, the T-Link module will supervise the communication with the panel. If option [3] is OFF and communication is lost with the panel, no trouble event will be transmitted from the T-Link to the receiver.

Default		Option ON	Option OFF
OFF	Option 1	Future Use	Disabled
ON	Option 2	Receiver Supervised	Disabled
ON	Option 3	Panel Supervised	Disabled
OFF	Options 4 to 8	Future Use	Disabled

[021] Programmable Output

To control the PGM output, program the following section with the correct option. When the selected condition occurs the PGM will trigger to ground for the duration of the trouble.

Default: 00

|_|_|

Options:
00 No Trigger
01 Receiver Absent
02 Panel Absent

[999] Default / Restart

Enter 00 to default the unit to factory settings.
Enter 55 to restart the unit.

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

4.3 T-Link Programming Section

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

Unique IP address for the module. The network administrator will provide this information.

Default: 000 000 000 000

[002] Subnet Mask

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.

Default: 000 000 000 000

[003] Receiver IP (Static IP address for the receiver)

Program the IP address of the central station receiver.

Default: 000 000 000 000

[004] T-Link Gateway

If the T-Link must communicate through a local gateway to connect with the receiver (WAN network), this is the IP address of the local gateway.

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

Default: 000 000 000 000

[007] T-Link Source Port Number

Default: 3060

[008] T-Link Destination Port Number

Default: 3061

2.1 Connecting the T-Link to the Panel

The power should be removed from the control panel before any connections are made to the T-Link. Connect the 12V and GND terminals to the panel's auxiliary power output. Connect the header cable from the T-Link's white panel connector to the PC-Link header of the control panel.

The black wire of the PC-Link cable is pin 1 on the Power864 PC5020 v3.2 or higher control panel PC-Link header. The PC-Link header on the MAXSYS PC4020 v3.31 or higher control panel will only accept the proper connection.

NOTE: *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 subscribers.*

2.2 Remote Control

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

NOTES: *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 dscsec.com/dls3drivers.htm.*
DLS-3 and System Administrator cannot communicate directly to the T-Link module. The T-Link must have The Reporter IP software or the SG-DRL-IP central station receiver line card to act as a communicator router to enable DLS or System Administrator communication.
The DLS software could be used with UL Listed installations only when a service personnel is on the site.

2.3 Programming

Programming must be done via the keypad on the DSC control panel. T-Link programming cannot be done using DLS software.

2.4 Unique IP Address

Each T-Link on the same network module must have a unique static IP address. This system is not compatible with any device that masks the IP address of the originating device. If such devices are present on the communication path the masking feature must be disabled for the T-Link modules. Since the MAC address of the unit is unique, this number can be used to create an exception rule.

2.5 Mounting the Module

For installation with the PC4020 control panel, refer to the PC4020 Installation Manual and the diagrams on Pages 12,13,14.

For installation with the PC5020 control panel, refer to the bracket (optional - sold separately) instructions for mounting the unit and the diagrams on Pages 12,13,14.

2.6 Hardware Features of Transmitter

2.6.1 LED

There are three LEDs on the board to indicate connection and traffic.

LED Diagnostics

LED1 Ethernet Transmit
LED2 Ethernet Receive
LED3 Ethernet Collision

Both LED1 and LED2 are normally ON in their default state after power-up (i.e., when no Ethernet cable is connected, and there are no packets being transmitted or received). When a packet is transmitted, LED1 will go off for a period of about 100ms, and then on again (it will blink once). When a packet is received, LED2 will go off for a period of about 100ms, and then on again (it will blink once). If both LED1 and LED2 are off after applying power, the T-Link is not operational.

2.6.2 Specifications

The maximum allowable current draw from the panel on the Auxiliary is 500 mA @ 12 VDC. Operational current draw of the T-Link is 150 mA.

The T-Link module has a switched negative programmable output (50 mA @ 12 VDC). This output can be activated if the T-Link module loses communication with the receiver **OR** with the panel.

- Input Voltage: 12 VDC
- Current: 150 mA (200 mA with PGM)
- Size: 3.25" × 5.25" (8.3 cm × 13.3 cm)
- Operating Temperature: 32°-122°F (0°-49°C)
- Output Protocols: TCP/IP 10 BaseT half duplex
- Input Protocols: PC-Link (SIA format)
- Connectors: 4-pin header for the PC-Link and RJ-45 for Ehternet
- Network: Ethernet LAN/WAN 10 BaseT or 10/100 BaseT
- Call Direction options: Primary or backup communicator
- Downloading support: Using DLS-3 and/or System Administrator software with The Reporter IP or DRL-IP line card
- Programming: Panel keypad
- Multiple Central Stations: Primary and backup via phone line*
- Approval Listings: FCC, IC, CE, UL and ULC

* The T-Link module is a single socket device which can only communicate with one network receiver.

NOTES: *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.

Step 10: After all T-Link 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 programming.

4.2 Programming via the PC5020 control panel

NOTE:*PC5020 Rev03 hardware required.*

Programming Steps:

Step 1: Program the hex digits [DCAA] in the telephone number that will be used for T-Link 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.

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

Step 5: Enter section [851] for T-Link 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 module in section [001].

Step 7: Program the subnet mask for the T-Link module in section [002].

Step 8: Program the static IP address of the receiver (DRL-IP line card or the PC running The Reporter IP software) in section [003].

Step 9: If the receiver (DRL-IP or The Reporter IP software) 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 [004]. This is an optional step; please discuss with the network administrator if this is required.

Step 10: Program section [020] 'System Status', option 2 'Receiver Supervised' OFF (disabled). This option should only be enabled when T-Link is being used for Canadian ULC level 3 installations.

Step 11: After all T-Link 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 programming.

NOTE:*The PC5020 T-Link 'Wait for Receiver Acknowledge' default is 20 sec. (programmed in [167]).*

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

1. The static IP address for the T-Link module. (Section [001])
2. The subnet mask for the T-Link module. (Section [002])
3. The static IP address of the receiver. (Section [003])
4. The static IP address of the static gateway for the LAN the T-Link is connected to in a WAN configuration. (Section [004])

Remember This: If you are using a telephone line to back up communication, be sure to program what phone number you want to use as a backup or dial direction option in section [000401] 'Communication Toggle Options'. If using a PC4020 or with a 5020 [380] option 5, enables 3rd number to backup. It is recommended that T-Link communication be programmed to transmit first as it is faster than land line communication. If the land line communication is programmed to communicate first, then the T-Link communication will be delayed for the duration of the land line call (about 30-45 seconds). The same idea should apply when using the phone line for backup only.

4.1 Programming via the PC4020 control panel

NOTE:*PC4020 Rev04B hardware required.*

Programming steps:

Step 1: Program the Hex digits [CAAA] in the telephone number that will be used for T-Link 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 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].

Step 7: Program the subnet mask for the T-Link module in section [002].

Step 8: Program the receiver static IP address (DRL-IP line card or the PC running The Reporter IP software) in section [003].

Step 9: If the receiver (DRL-IP or The Reporter IP software) 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 [004]. This is an optional step; please discuss with the network administrator if this is required.

To simplify bench testing and increase diagnostic ability, it is often beneficial to connect the T-Link and the receiver directly to each other, using an Ethernet crossover cable (see Section 3.2 "Making an Ethernet Crossover Cable"). The diagnostic information for use with a crossover cable is outlined in this section.

Upon T-Link power-up (without the Ethernet cable connected), LED1 will blink periodically, approximately once every 12 seconds. This represents the T-Link attempting to send a TCP/IP socket connection request to the receiver. The T-Link will try to connect to the receiver until it succeeds. At the same time, LED2 will remain solid ON indicating that no packets are being received. If both LEDs do not exhibit this behavior, the T-Link is NOT functioning properly.

3.1 Troubleshooting

If the receiver (either The Reporter IP or the DRL-IP) is properly configured, within a few seconds of connecting the Ethernet cable LED2 will blink once, after which both LED1 and LED2 will enter a steady ON state. This represents a successful TCP/IP socket connection with the receiver. At this point, The Reporter IP or the DRL-IP will be able to report that the T-Link is connected. Any subsequent alarm messages or other transmissions will result in both LED1 and LED2 blinking once each, simultaneously, for each message sent. This behavior represents the original message being sent/received and a response (i.e., an ACK) being received/sent.

If LED1 continues to blink once every 12 seconds, and LED2 remains on, this signifies that no communication can be established with the receiver. In this case the receiver is not responding and accepting the socket connection request from the T-Link. This can be caused by the receiver not being powered, faulty cabling, or incorrect T-Link configuration (incorrect T-Link IP address, subnet mask, gateway, or receiver IP address).

If LED1 continues to blink once every 2 seconds, and LED2 also blinks once every 2 seconds, more or less in unison, this represents a problem either with the receiver or the T-Link configuration. As an example, if the T-Link is connected to a PC with The Reporter IP installed, but The Reporter IP application is not running at that instant, this is the LED behavior that will be seen (assuming all other configuration information is correct). If The Reporter IP or DRL-IP is running, this could indicate an improper port setting in either the T-Link or DRL-IP. It could also indicate an improper receiver IP address, signifying that the address entered into the T-Link is actually the address of another host on the network.

3.2 Making an Ethernet Crossover Cable

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

3.3 Call Direction

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

3.4 Port Usage Table

NOTE: *Please confirm with the network administrator that the following ports are locked open and that the PC running The Reporter IP has network access for all required network segments.*

Description		Default Port #	Programming Location to Change
T-Link	T-Link Source Port	3060	Section [007] T-Link options from Keypad
	T-Link Destination Port	3061	Section [008] T-Link options from Keypad
The Reporter IP	T-Link Port	3061	Configuration menu
	DLS Port	3062	Configuration menu
	SA Port	3063	Configuration menu
DRL-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	3060	Section [14] [15] from Console S/W
DLS-3	DLS Port	3062	Modem Configuration Options
DLS SA	SA Port	3063	Modem Configuration Options

Before You Get Started

You will need to obtain the following information from the Network Administrator for the LAN/WAN on which you are installing T-Link communication.

3.5 Network Address Worksheet

3.5.1 Receiver Line Cards

Line Card	Static IP	Subnet Mask	Receiver	Receiver #	Receiver Line #
Default:	000.000.000.000	000.000.000.000	000.000.000.000	00	000
DRL IP #1					
DRL IP #2					
DRL IP #3					
DRL IP #4					
DRL IP #5					
DRL IP #6					
DRL IP #7					
DRL IP #8					
DRL IP #9					
DRL IP #10					
DRL IP #11					
DRL IP #12					
DRL IP #13					
DRL IP #14					
DRL IP #15					

3.5.2 PC#1 (The Reporter IP)

PC Network Name	Static IP Address	Subnet Mask	Network Location	Receiver Number	Line Number
(Enter name here)	(000.000.000.000)	(000.000.000.000)	(Enter location here)	(02)	(001)

3.5.3 PC#2 (DLS/SA)

PC Network Name	Network Location
(Enter name here)	(Enter location here)

3.5.4 PC#3 (DLS/SA)

PC Network Name	Network Location
(Enter name here)	(Enter location here)

3.5.5 T-Link Accounts

Line Card Module #	Static IP Address	Subnet Mask	Panel Account #	Receiver IP	T-Link Gateway
Default:	000.000.000.000	000.000.000.000	AAAA	000.000.000.000	000.000.000.000
T-Link #001					
T-Link #002					
T-Link #003					
T-Link #004					
T-Link #005					
T-Link #xxx					
T-Link #xxx					
T-Link #255					