

Sur-Gard System III

SG-DRL3-IP

Receiver Line Card



Installation & Operating Manual version 2.2



WARNING: *This manual contains information on limitations regarding product use and function and information on the limitations as to liability of the manufacturer. The entire manual should be carefully read.*

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/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, barbecues, 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 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.

Products which Digital Security Controls determines not to be repairable will be replaced by the nearest equivalent product available at that time. The current market price of the replacement product will be charged for each replacement unit.

Table of Contents

Section 1 - Introduction.....	1 1
1.1 Features	1
1.2 Support Software.....	1
System III 2.1 System III Console Software.....	1
1.2.2 T-LINK Console Software	1
1.3 System Overview	1
1.4 Approvals	2
1.5 Receiver Setup and Operation.....	2
1.6 Description (Operation).....	3
1.6.1 Operation with Default Programming.....	3
1.6.2 Virtual Connectivity.....	4
1.6.3 Status Addressing.....	4
1.6.4 Automation input/output (Port 1025).....	4
1.6.5 Automation Protocols.....	4
1.6.6 Data Byte Protocol.....	4
1.6.7 Acknowledgment of the Signal.....	4
1.6.8 Automation Responses.....	4
1.6.9 Automation Absent.....	4
1.6.10 System III SIA Internal Status Output	4

Section 2 - Operating Modes	5
2.1 SG-DRL3-IP Standby Mode.....	5
2.2 CPM3 Error	5
2.3 Fault Data Message.....	5
2.4 Ethernet Interface.....	5
2.5 ULAA Receiver Database	5
2.6 SG-DRL3-IP Debug Output	5
Section 3 - SG-DRL3-IP Programming.....	6
3.1 Options: [00] - [47].....	6
Glossary.....	9
Appendix A - CPM3 Internal Status Messages	12
Appendix B - DVACS Events.....	12
Appendix C - SG-DRL3-IP Events	13
Appendix D - DEC-HEX-BIN Conversion Chart	14
Appendix E - ASCII Character Chart	14
Appendix F - DVACS Alarm Flow Comparison: SG-DVL2A Configuration / SG-DRL3-IP Configuration	15
Appendix G - T-LINK TL300 Contact ID Reports.....	15

IMPORTANT - READ CAREFULLY:

DSC Software purchased with or without Products and Components is copyrighted and is purchased under the following license terms:

- This End-User License Agreement ("EULA") is a legal agreement between **You** (the company, individual or entity who acquired the Software and any related Hardware) and **Digital Security Controls, a division of Tyco Safety Products Canada Ltd.** ("DSC"), the manufacturer of the integrated security systems and the developer of the software and any related products or components ("HARDWARE") which You acquired.
- If the DSC software product ("SOFTWARE PRODUCT" or "SOFTWARE") is intended to be accompanied by HARDWARE, and is NOT accompanied by new HARDWARE, You may not use, copy or install the SOFTWARE PRODUCT. The SOFTWARE PRODUCT includes computer software, and may include associated media, printed materials, and "online" or electronic documentation.
- Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to You under the terms of that license agreement.
- By installing, copying, downloading, storing, accessing or otherwise using the SOFTWARE PRODUCT, You agree unconditionally to be bound by the terms of this EULA, even if this EULA is deemed to be a modification of any previous arrangement or contract. If You do not agree to the terms of this EULA, DSC is unwilling to license the SOFTWARE PRODUCT to You, and You have no right to use it.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE This EULA grants You the following rights:

- (a) **Software Installation and Use** - For each license You acquire, You may have only one copy of the SOFTWARE PRODUCT installed.
- (b) **Storage/Network Use** - The SOFTWARE PRODUCT may not be installed, accessed, displayed, run, shared or used concurrently on or from different computers, including a workstation, terminal or other digital electronic device ("Device"). In other words, if You have several workstations, You will have to acquire a license for each workstation where the SOFTWARE will be used.
- (c) **Backup Copy** - You may make back-up copies of the SOFTWARE PRODUCT, but You may only have one copy per license installed at any given time. You may use the back-up copy solely for archival purposes. Except as expressly provided in this EULA, You may not otherwise make copies of the SOFTWARE PRODUCT, including the printed materials accompanying the SOFTWARE.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

- (a) **Limitations on Reverse Engineering, Decompilation and Disassembly** - You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to the Software, without the written permission of an officer of DSC. You may not remove any proprietary notices, marks or labels from the Software Product. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA.
- (b) **Separation of Components** - The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one HARDWARE unit.
- (c) **Single INTEGRATED PRODUCT** - If You acquired this SOFTWARE with HARDWARE, then the SOFTWARE PRODUCT is licensed with the HARDWARE as a single integrated product. In this case, the SOFTWARE PRODUCT may only be used with the HARDWARE as set forth in this EULA.
- (d) **Rental** - You may not rent, lease or lend the SOFTWARE PRODUCT. You may not make it available to others or post it on a server or web site.
- (e) **Software Product Transfer** - You may transfer all of Your rights under this EULA only as part of a permanent sale or transfer of the HARDWARE, provided You retain no copies, You transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades and this EULA), and provided the recipient agrees to the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade, any transfer must also include all prior versions of the SOFTWARE PRODUCT.
- (f) **Termination** - Without prejudice to any other rights, DSC may terminate this EULA if You fail to comply with the terms and conditions of this EULA. In such event, You must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.
- (g) **Trademarks** - This EULA does not grant You any rights in connection with any trademarks or service marks of DSC or its suppliers.

- 3. **COPYRIGHT** - All title and intellectual property rights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, and text incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by DSC or its suppliers. You may not copy the printed materials accompanying the SOFTWARE PRODUCT. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE PRODUCT are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants You no rights to use such content. All rights not expressly granted under this EULA are reserved by DSC and its suppliers.

- 4. **EXPORT RESTRICTIONS** - You agree that You will not export or re-export the SOFTWARE PRODUCT to any country, person, or entity subject to Canadian export restrictions.

- 5. **CHOICE OF LAW** - This Software License Agreement is governed by the laws of the Province of Ontario, Canada.

- 6. **ARBITRATION** - All disputes arising in connection with this Agreement shall be determined by final and binding arbitration in accordance with the Arbitration Act, and the parties agree to be bound by the arbitrator's decision. The place of arbitration shall be Toronto, Canada, and the language of the arbitration shall be English.

7. LIMITED WARRANTY

- (a) **NO WARRANTY** - DSC PROVIDES THE SOFTWARE "AS IS" WITHOUT WARRANTY. DSC DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

- (b) **CHANGES IN OPERATING ENVIRONMENT** - DSC shall not be responsible for problems caused by changes in the operating characteristics of the HARDWARE, or for problems in the interaction of the SOFTWARE PRODUCT with non-DSC-SOFTWARE or HARDWARE PRODUCTS.

- (c) **LIMITATION OF LIABILITY; WARRANTY REFLECTS ALLOCATION OF RISK** - IN ANY EVENT, IF ANY STATUTE IMPLIES WARRANTIES OR CONDITIONS NOT STATED IN THIS LICENSE AGREEMENT, DSC'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS LICENSE AGREEMENT SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU TO LICENSE THE SOFTWARE PRODUCT AND FIVE CANADIAN DOLLARS (CAD\$5.00). BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

- (d) **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 DSC. DSC MAKES NO OTHER WARRANTIES. DSC NEITHER ASSUMES 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 SOFTWARE PRODUCT.

- (e) **EXCLUSIVE REMEDY AND LIMITATION OF WARRANTY** - UNDER NO CIRCUMSTANCES SHALL DSC BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT 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 SOFTWARE PRODUCT OR ANY ASSOCIATED EQUIPMENT, COST OF CAPITAL, COST OF SUBSTITUTE OR REPLACEMENT EQUIPMENT, FACILITIES OR SERVICES, DOWN TIME, PURCHASERS TIME, THE CLAIMS OF THIRD PARTIES, INCLUDING CUSTOMERS, AND INJURY TO PROPERTY. **WARNING: DSC 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 SOFTWARE PRODUCT to fail to perform as expected.**

GENERAL DESCRIPTION of the EQUIPMENT and CLASSIFICATION.

CLASSIFICATION

The SYSTEM III equipment is a CLASS 1, RACK-MOUNTED, (FIXED – STATIONARY) EQUIPMENT, PLUGGABLE TYPE A USING A DETACHABLE POWER SUPPLY CORD, designed to be INSTALLED, OPERATED and MAINTAINED by SERVICE PERSONNEL ONLY [persons having appropriate technical training and experience necessary to be aware of hazards to which they are exposed in performing a task and of measures to minimise the danger to themselves or other persons].

The equipment SYSTEM III is designed to be installed in RESTRICTED ACCESS LOCATIONS within an environment that provides the Pollution Degree max 2 and OVERVOLTAGES CATEGORY II - NONHAZARDOUS LOCATIONS, INDOOR ONLY.

The POWER SUPPLY CORD serves as a means of disconnection from the MAINS. The OUTLET used to power the equipment shall be installed near the equipment and shall be easily accessible. The equipment must be connected to a socket-outlet with a protective earthing connection! The INSTALLATION of the SYSTEM III equipment must provide a reliable earth connection and it shall respect the local electrical wiring regulations.

IMPORTANT:

IT IS THE RESPONSIBILITY OF THE INSTALLER TO ENSURE THAT THE SYSTEM III EQUIPMENT IS PROPERLY MOUNTED WITHIN A METALLIC FIRE ENCLOSURE WITH A MINIMUM THICKNESS OF 1.5 mm AND THE FINAL ASSEMBLY IS COMPLIANT with ALL OF THE APPLICABLE REQUIREMENTS FROM THE POINT OF VIEW OF THE ACCESSIBILITY TO THE ENERGIZED PARTS (HAZARDOUS VOLTAGES, TNV CIRCUITS, ETC.) AS THESE CHARACTERISTICS ARE DEFINED WITHIN THE EN60950:2000 STANDARD.

THE EXTERNAL ENCLOSURE SHALL MEET ALL OF THE APPLICABLE REQUIREMENTS FROM THE POINT OF VIEW OF PHYSICAL REQUIREMENTS, e.g.: STEADY FORCE 250N, IMPACT AND STABILITY. THE EQUIPMENT MUST BE SECURED TO THE BUILDING STRUCTURE BEFORE OPERATION; ALL WIRING AND INSTALLATION SHALL BE IN ACCORDANCE WITH ELECTRICAL CODES ACCEPTABLE TO THE AUTHORITIES THAT HAVE JURISDICTION WHERE THE EQUIPMENT IS INSTALLED, SERVICED AND OPERATED.

NOT MORE THAN 3 (THREE) ASSEMBLIES [EACH CONSISTING OF 2 (two) System III EQUIPMENT] MOUNTED WITHIN THE SAME RACK SHALL BE POWERED FROM THE SAME BRANCH CIRCUIT. USE A DIFFERENT BRANCH CIRCUIT FOR ANY GROUP LARGER THAN 3 (THREE) ASSEMBLIES.

Internal wiring shall be routed in a manner that prevents:

- excessive strain on wire and on terminal connections;
- loosening of terminal connections;
- damage of conductor insulation.

The wireways within the enclosure shall be smooth and free from sharp edges. Wires shall be protected and routed so that they do not come in contact with burrs, cooling fan or heatsinks which could cause damage to the insulation of conductors. Holes in metal shall have smooth well-rounded surfaces or shall be protected with bushings.

The EXTERNAL ENCLOSURE shall be connected to the PROTECTIVE EARTH GROUND. The external cabinet (RACK) must be secured to the building structure before operation in a such a way to fully meet the STABILITY REQUIREMENTS as per EN60950: 2000 conditions.

An adequate MARKING [visible before the door (cover)], NEXT TO THE ACCESS DOOR (or cover) of the rack, with instructions for protection once the DOOR (or covers) IS (are) removed, stating that “telephone cord is to be disconnected prior to opening the door” is an example of an acceptable Marking), and it shall be provided by the Installer.

An acceptable power supply cord (detachable), shall be used accordingly to the local outlets and voltages. IT IS THE INSTALLER'S RESPONSIBILITY TO PROVIDE AN APPROPRIATE ACCEPTABLE POWER SUPPLY CORD.

CAUTION:

This product uses Lithium Batteries. Improper handling of lithium batteries may result in HEAT GENERATION, EXPLOSION or FIRE, which may lead to personal injuries.

Please ensure that the above precautions are strictly observed by the related divisions including but not limited to sales, service, customers and (or) outside contractors.

THE EQUIPMENT SYSTEM III IS EQUIPPED WITH LITHIUM NON REPLACEABLE BATTERY. DO NOT ATTEMPT TO REPLACE THE BATTERIES.

CONNECTION TO THE MAINS

1. Connect first the DETACHABLE POWER SUPPLY CORD to the IEC 320 connector located on SYSTEM III equipment.
2. Connect all the telecommunications cord-sets to the appropriate connectors.
3. Be sure that the enclosure of the equipment SYSTEM III is fully installed (covers, doors, etc.) in a such a way that HAZARDOUS VOLTAGES and TNV Circuits will not be ACCESSIBLE when the equipment will be connected to the MAINS and/or TELECOMMUNICATION NETWORK.

ATTENTION: THE INTERNAL POWER SUPPLIES ARE NOT SWAPPABLE! DISCONNECT POWER BEFORE ATTEMPTING TO CHANGE A POWER SUPPLY!

In order to change the INTERNAL Power Supply, first DISCONNECT the DETACHABLE POWER SUPPLY CORD from the socket outlet used to provide power, and then, from the IEC320 Connector which is mounted on the SYSTEM III equipment. Wait minimum 5 seconds to allow the Capacitor (C8) within the unit to discharge. IF THE FUSE IS SUSPECTED OF HAVING OPENED, a discharge path for the involved Capacitor (C8) shall be provided.

Do not touch the HEATSINKS within the equipment: these are LIVE PARTS and/or may present a hazard related to high temperatures. In order to swap the boards USE THE PROVIDED PLASTIC HANDLES (INSERTERS, EXTRACTORS).

NO REPAIRS IN THE FIELD ARE ALLOWED. THE EQUIPMENT SYSTEM III MUST BE RETURNED TO THE MANUFACTURER FOR REPAIRS.

Section 1 - Introduction

1.1 Features

The SG-DRL3-IP performs similar functions to the SG-DRL3 line card.

The SG-DRL3 line card receives alarm information from a control panel over a telephone line. The SG-DRL3-IP line card receives alarm information from panels over a LAN/WAN or internet network.

The System III receiver can be configured to use SG-DRL3 line cards, SG-DRL3-IP line cards or a combination of the two. Refer to the *System III Installation Manual* for additional information.

SG-DRL3-IP line card features include the following:

- Provides higher line security than conventional dial up panels with the polling feature.
- Quicker transmission since dialing or handshaking is not required.
- The control panel is the originator of the signals and as such will be the one requesting the ACK from the central station.
- Network trouble detection is displayed on LCD/Printer and automation software.
- Disconnect trouble detection.
- Static IP for programming of the network protocols.
- Data network polling environment for replacement of an existing DVACS network. Meets the 90 second ULC requirement for this option.
- SIA event descriptors are used when transmitting information to the central station from the control panel through the PC-Link connection.
- A security function communicates to the central station when a module is removed and replaced.

NOTES: The SG-DRL3-IP can only receive data from the following transmitters.

TL150	TL250*	TL250DV	TL300*	GS3055*
GS3060*	TL26X*	GS206X*	TL210	GS31XX

* UL/ULC Listed

The SG-DRL3-IP Receiver Module is **NOT** compatible with the T-LINK TL100.DVACS support on the T-LINK TL250/TL300 v1.10 or higher is only compatible with the SG-DRL3-IP v1.1x or higher.

The T-LINK TL300 Contact ID is only compatible with the SG-DRL3-IP V1.2x or higher.

1.2 Support Software

1.2.1 System III Console Software

The line card options must be changed through the CPM3 or using System III Console v2.30 (or higher) Software. The System III Console software provides support for the SG-DRL3 and SG-DRL3-IP line cards. Refer to the *SG-System III Installation Manual* for details.

1.2.2 T-LINK Console Software

The T-LINK Console v1.20 software is a stand-alone application that provides centralized support for the management and control of TL250/TL300 product line and SG-DRL3-IP line cards including:

- Generation and deployment of unique encryption keys to IP Receivers.
- Remote setup, control and TCP/IP configuration of the SG-DRL3-IP and T-LINK TL250/TL300 accounts.

- Local and remote programming of T-LINK TL250/TL300 devices.
- Software updates to T-LINK TL250/TL300 devices using TFTP (Trivial File Transfer Protocol).
- The T-LINK Console v1.20 updates T-LINK TL250/TL300 using TFTP session
- The T-LINK accounts table and data encryption keys will be stored in the local database.

Refer to the *T-LINK Console User Manual* for details.

1.3 System Overview

The SG-DRL3-IP (UDP) Receiver Module functions as a LAN or WAN server to many remote clients (the transmitters). The SG-DRL3-IP receiver module receives alarm events from the transmitter/panel (or from the transmitter when the transmitter is in standalone mode) and forwards them to the CPM3 for subsequent output to the printer and automation outputs.

After a receiver module has been configured and installed, it will run on a predefined port and await communications from transmitters which have been configured to connect to that specific receiver. When communication has been established, the transmitter will enter its normal operating mode (waiting for panel polls, transmit heartbeat signals, alarm messages and DLS/SA download messages). The SG-DRL3-IP will log the connection and generate the appropriate connection event for forwarding to the CPM3.

When an alarm message is generated, the transmitter will send the message in a UDP/IP/Ethernet frame and pass it along to the receiver (this communication can be optionally encrypted - reference transmitter documentation to determine if encryption is supported by the device). When an alarm message is received from the transmitter/panel, the receiver will strip off the UDP/IP/Ethernet frame and decrypt the message. It will then send an appropriate response (ACK or NAK) back to the transmitter/panel. The timing will follow the standard timing requirements of the panel. If the message was a valid alarm event, the event will be sent to the appropriate connected printer and automation devices.

The SG-DRL3-IP Receiver Module receives heartbeats from all network supervision enabled transmitters periodically. This allows the receiver to determine whether the transmitters are still online. The receiver maintains a table of all installed transmitters and monitors their status (presence/absence, installed software versions, MAC addresses for swap detection purposes, and other network statistics).

The SG-DRL3-IP Receiver Module can be programmed with various configuration parameters and options, including receiver IP address, receiver sub net mask, and default gateway address. Configuration parameters are password protected. The default password can be changed during initial installation for maximum security.

The SG-DRL3-IP Receiver Module is programmed with a globally unique MAC address during production. This MAC address is NOT re-programmable.

NOTE: Each SG-DRL3-IP Receiver Module can monitor up to a maximum of 1536 account of which 512 accounts can be supervised.

1.4 Approvals

1.4.1 Industry Approvals

- UL 1610 Central Station Burglar Alarm Units
- UL 864 Standard for Control Units and Accessories for Fire Alarm Systems
- CAN/ULC-S304-06 Signal Receiving Centre and Premises Burglar Alarm Control Units
- CAN/ULC-S559-04 Equipment for Fire Signal Receiving Centres and Systems
- EN60950-1:2001 Standard for Information Technology Equipment.
- AS/NZS 60950:2000 Information Technology Equipment - Safety
- CISPR22 Information Technology Equipment - Radio Disturbance Characteristics - Limits and Methods of Measurements

- EN50130-4 Immunity requirements for components of fire, intruder and social alarm systems.

This equipment shall be installed in accordance with the requirements of NFPA72, NFPA70, UL827 and the authority having jurisdiction.

SG-System III with SG-DRL3-IP Line Card is ULC listed for active communication channel security level A4 when used in conjunction with T-Link TL250 and T-Link TL300 Internet/Intranet alarm communicators. For this type of application the supervision and encryption features have to be enabled.

For ULC Installations the equipment shall be installed in accordance with the requirements of ULC-S561 and ULC-S301 Standards and the authority having jurisdiction.

UL864 Programming Requirements

Table 1-1: UL864 Programming Requirements

NOTICE to Users, Installers, Authorities having Jurisdiction, and other involved parties					
This product incorporates field programmable software. In order for the product to comply with the requirements in the Standard for Control Units and Accessories for Fire Alarms Systems , UL 864, certain programming features or options must be limited to specific values or not used at all as indicated below.					
Opt #	Program Option	Page	Permitted in UL 864? (Y/N)	Possible Settings	Settings Permitted (UL 864)
13-14	TX ABSENT DEBOUNCE TIME - - - - -	6	N	1E - FFH (30-255)	05AH(90s)
15-16	TX ABSENT RESTORE TIME - - - - -	6	N	1E - FFH (30-255)	05AH(90s)
17	MASK NETWORK PRESENT - - - - -	6	N	ON/OFF	OFF
18	MASK NETWORK ABSENT - - - - -	6	N	ON/OFF	OFF
19	MASK TX RESTORAL - - - - -	7	N	ON/OFF	OFF
1A	MASK TX FAILURE - - - - -	7	N	ON/OFF	OFF
1B	MASK TX SWAP - - - - -	7	N	ON/OFF	OFF
1C	MASK TX UNENCRYPTED - - - - -	7	N	ON/OFF	OFF
1D	MASK INVALID REPORT - - - - -	7	N	ON/OFF	OFF
1E	MASK UNKNOWN ACCOUNT - - - - -	7	N	ON/OFF	OFF
1F	MASK ACCOUNT EXCEEDED - - - - -	7	N	ON/OFF	OFF
21	MASK OPTION CHANGE - - - - -	7	N	ON/OFF	OFF
2B	BUSY OUT - - - - -	8	N	00-05	00

1.5 Receiver Setup and Operation

DSC recommends testing the receiver before actual installation. Becoming familiar with the connections and setup of the unit on the workbench will make final installation more straightforward. The following items are required:

- IEC Power supply cord
- One network hub or router
- One or more dialer or digital control panel and a T-LINK TL250/TL300

1. Unpack the components for the System III.

NOTE: Carefully unpack the receiver and inspect for shipping damage. If there is any apparent damage, notify the carrier immediately.

2. Unscrew the front thumb screws and open the front plates.

NOTE: Before inserting the CPM3, connect the ribbon cable from the UIB3 board. Before inserting the PSC3 connect the LCD backlight.

3. Insert all the cards in the rack, in their appropriate position. Refer to Figure 1-2 in the System III Installation Manual.

Connect the ribbon cable of the front panel to the CPM3 before inserting it. Connect the backlight power connection to the PSC3 then insert the PSC3.

4. Insert the PSU3 into the rack and fasten it properly.
5. Connect an ethernet cable to the proper line card.
6. Connect the main power (110VAC or 220VAC) using a standard computer IEC cable (not supplied).
7. The LCD will power up and display internal troubles (printer, computer, telephone line fault, network absent). The SG-DRL3-IP Receiver will have the green LED ON if the ethernet line is connected. If the LED is not on, make sure the ethernet line is connected to the right port.

NOTE: Internal diagnostics may require more than one minute during the power up sequence.

8. Send a signal from a control panel to the receiver. The signal will be displayed on the LCD. Press the [ACK] button to silence the buzzer.

Figure 1, SG-DRL3-IP Layout

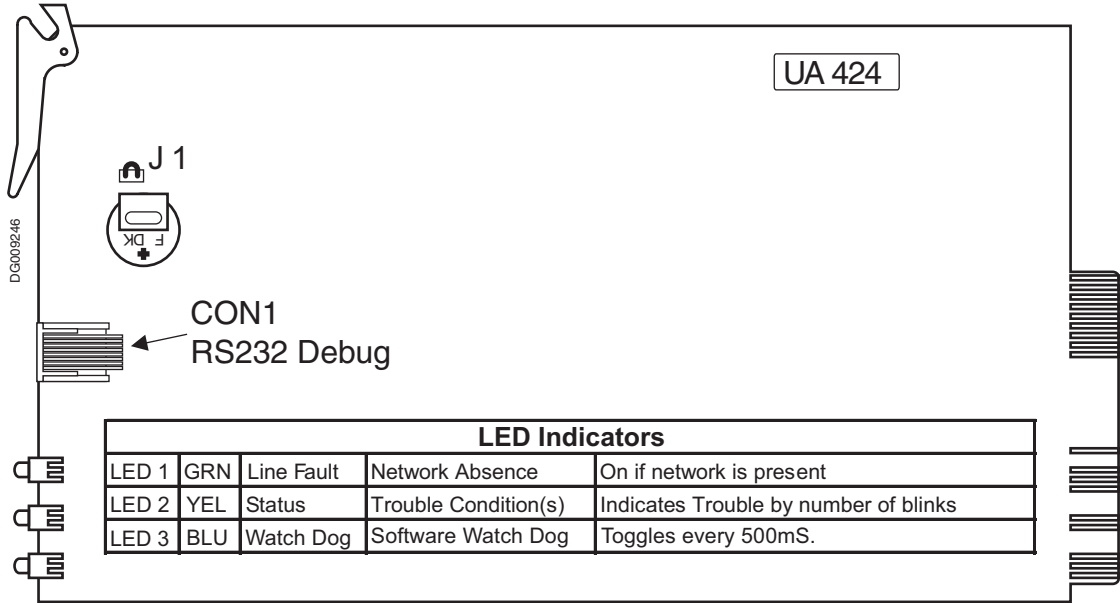


Figure 2, System III Wiring Diagram

* For Model System III CE:

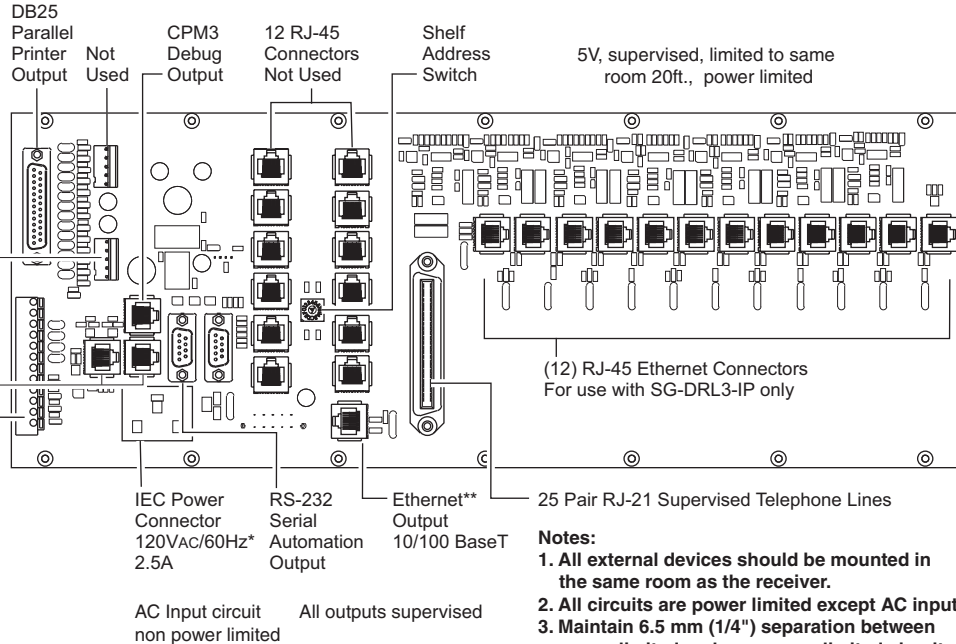
- 240VAC /50Hz
- System III CE is not UL Listed

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

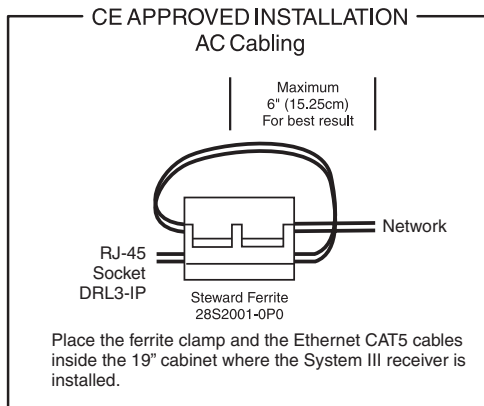
Connections for second backplane

See System III Supervised UPS Connection Diagram for details

Note: For UL Installations
AC input is 120VAC/60Hz.
Do not connect to a receptacle controlled by a switch.



- Notes:**
1. All external devices should be mounted in the same room as the receiver.
 2. All circuits are power limited except AC input.
 3. Maintain 6.5 mm (1/4") separation between power limited and non-power limited circuits.



NOTE: When a hub or router/gateway is used in conjunction with the System III receiver, 24-hr standby power is required for these devices (i.e., UL Listed UPS, battery backup or engine driven generator).

1.6 Description (Operation)

1.6.1 Operation with Default Programming

Without any changes to the factory default programming, the receiver operates as indicated below:

- The signals are sent to the parallel printer and computer connected to serial port COM1 or to the 10/100BaseT connector.
- If a computer is not connected, press the [ACK] button on the CPM3 to silence the buzzer and to clear the alarm from the LCD display.

1.6.2 Virtual Connectivity

Each receiver has one IP address and a number of associated ports. Internal socket programming uses specific ports for expected tasks. The configuration management, done from the Console Software, is located on port 1024. The System III Console software is provided for Windows 98/ME/NT/2000/XP, which provides a graphical style menu for configuration management. Additional features are available with the console software including storage of virtual receiver setups, and configuration wizards.

1.6.3 Status Addressing

Line card status is reported via physical addressing. Shelf and slot number are assigned automatically to each line card. All device status information is in Sur-Gard format. The reporting of status on this port, automation output and printer will relate to physical addressing.

1.6.4 Automation input/output (Port 1025)

Traditional automation communication is provided via port 1025 on the Ethernet connection. This primary port is a Sur-Gard standard output and provides Sur-Gard standard automation output. All or a number of virtual receiver types could be mapped to the Sur-Gard output.

1.6.5 Automation Protocols

The Sur-Gard System III receiver sends a variety of protocols to report signals to the central station computer via a TCP/IP and/or RS-232 port. A complete list of protocols can be provided upon request.

1.6.6 Data Byte Protocol

The Sur-Gard System III receiver uses a default configuration of 9600 Baud rate, 1-start bit, 8-data bits, 0-parity bits and 2-stop bits structure, to transmit and receive signals on the RS-232 port. This protocol can be programmed on the receiver to enable different configurations.

1.6.7 Acknowledgment of the Signal

The Sur-Gard System III receiver requires an acknowledgment signal [ACK] (Hex 06) from the computer software within 4 seconds for each message sent. Failure to receive the [ACK] will result in 3 retransmissions of the signal before indicating a communication failure. During a communication failure the System III receiver will cease transmitting except for the heartbeat. The same thing happens if the receiver receives a [NAK] (Hex 15). In case of communication failure with the computer, the System III DRL3 line card can store up to 512 events and the DRL3-IP line card can store up to 768 events in the line card internal memory. Communication is resumed when the first acknowledgment is received on the heartbeat; all buffered information is then transmitted.

1.6.8 Automation Responses

When the CPM3 sends an event to the computer, it checks for 3 responses: ACK, NAK or Unknown/No Response. An ACK tells the CPM3 the computer automation got the event successfully. A NAK tells the CPM3 the computer automation got the messages but didn't understand it.

The line card will attempt to send the messages 25 times. If after 25 attempts it continually gets a NAK from the computer automation, the CPM3 will send an internal communication error event to the printer. After 25 attempts, the line card will send an internal communication event to the printer, and then begin attempting to send the next event in the line card buffer to the computer automation.

Any other response from the computer automation, including no response will cause the CPM3 to attempt to send the message again, up to 4 times. If after 4 attempts the CPM3 gets no response or an unknown response, it will assume nothing is connected and generate an alarm.

1.6.9 Automation Absent

When the computer is not responding to transmissions, the CPM3 will generate a 'SG-Serialx fail' or 'SG-TCP/IPx Fail' trouble. When a trouble occurs, the CPM3 will continue to attempt to send a heartbeat signal to the computer until it gets a response. The System III receiver will make 4 attempts, then wait for the next heartbeat period before making another 4 attempts. The typical heartbeat interval is 30 seconds..

Supervisory Heartbeat Signal Protocol (1)

100000ssssssssss@ssss[DC4]	
00000	Receiver number (Real programmed number Never virtual).
S	Space Character.
@	Supervisory Signal.
[DC4]	Terminator, 14 Hex

This signal is used to supervise the communication between the receiver and computer automation. It is sent to the computer automation every 30 seconds and is programmable from the receiver. The computer automation should acknowledge this signal with an [ACK]. The CPM3 can be programmed to send a test signal to the computer automation once every 01-99 seconds to test the connection between the CPM3 and the computer automation (30 seconds is recommended). If a heartbeat fails to get a response from the computer automation, the CPM3 will immediately transmit the heartbeat again, up to 4 attempts. If all computer automation output fails and if by default the TCP/IP automation fails, the CPM3 will switch to the serial automation output.

If the output fails, the CPM3 will switch to manual mode, all signals will be displayed on the LCD and will require a manual acknowledge. To re-establish connection with the TCP/IP a reset fallback command must be generated from the Console software. If the line card buffers are full, the line cards will stop answering the calls.

1.6.10 System III SIA Internal Status Output

O	ORRLLL[#0000 NYZZZZ] Protocol ID
RR	Receiver number of the CPM3
LLL	000 signifies a CPM3 Event.
0000	System III Account.
NYZZ	SIA Event
[DC4]	Terminator, 14 Hex

ORRLLL[#0000|NYZZZZ]: RR is the receiver number of the CPM3, and LLL will be 000 to signify a CPM3 event. Refer to **Appendix A: CPM3 Internal Status Messages**.

Section 2 - Operating Modes

2.1 SG-DRL3-IP Standby Mode

After start-up the line card enters the Standby mode and monitors the network connection and the CPM3. Depending on the system's status, the following conditions will be displayed for each line card:

12	LED	ON	OFF	FLASHING
	LINE (Green)	Network Present	Network Absent	N/A
	STATUS (Yellow)	Trouble Condition(s)	Off-line	*Error condition
	WATCHDOG (Blue)	Line Card not functional		Line Card functional

*The number of flashes on the yellow LED indicates the following errors:

Flashes	Error
1	CPM Absent
2	Line Card Busy
3	Printer Buffer Full
4	Computer Buffer Full
5	Checksum Failed

2.2 CPM3 Error

If the SG-DRL3-IP cannot detect the CPM3 polling, the SG-DRL3-IP will start buffering incoming calls. Up to 768 alarm messages for the printer and computer will be retained in the SG-DRL3-IP event buffer. When the event buffer is full, the line card will stop processing alarms and the status LED will begin flashing. When the CPM3 error condition is corrected, the alarm messages in the event buffer will be transmitted to the CPM3 with the corresponding time/date the alarms have been received.

2.3 Fault Data Message

When this problem is encountered, the following information is transmitted to the printer and the computer:

Printer:

SG-12-234-AAAAAA-YN-*Invalid Report 192.158.8.34*

Computer:

012234[#AAAAAA;NYN*192.158.8.34*]

NOTE: This output for account code 'AAAAAA' indicates that data has been received, but is not valid (e.g., The packet is encrypted and the SG-DRL3-IP does not have the proper key) or the T-LINK transmitter packet was rejected (NAK) four times by the receiver. Please also refer to Option 45.

2.4 Ethernet Interface

The SG-DRL3-IP has an Ethernet interface which operates as a 10BaseT/100BaseT IEEE 802.3 compliant Ethernet port (half duplex mode). This port is accessible via a standard RJ45 connector. A LINK plus ACTIVITY LED is also present on the board for diagnostics and troubleshooting. The IP address of the SG-DRL3-IP is programmable. The ethernet port is used for system connections, including the transmitter and console ports.

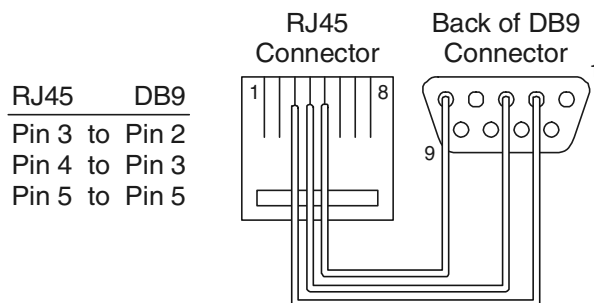
CAUTION: The ethernet communication lines must be connected first to an approved (acceptable to the local authorities) type NID (Network Interface Device) before leaving the premises (e.g., *UL installations, UL60950 Listed NID*).

2.5 ULAA Receiver Database

The receiver has the capability of monitoring T-LINK transmitters that are setup as ULAA units. The receiver will automatically keep track of new transmitters and indicate whenever a transmitter has been lost. No option is required on the receiver since if no ULAA heartbeat signals are received then the receiver will function normally. Refer to **Appendix C: SG-DRL3-IP Events**.

2.6 SG-DRL3-IP Debug Output

Connect the RJ45 end of the debug cable to the debug output jack on the front of the line card. Connect the female DB9 connector to the serial port of a computer (COM1 or COM2 port - usually DB9 male. Refer to the *System III Installation Manual* for details.



Section 3 - SG-DRL3-IP Programming

NOTE: System III Console v2.20 (or higher) software is required for programming and communication with SG-DRL3-IP Receiver Modules.

3.1 Options: [00] - [47]

✓ *Indicates Default*

Option [00]: For future use

Options [01] - [04]: Receiver IP Address

This IP address identifies the SG-DRL3-IP on the IP network. Each node on the IP network must be assigned a unique IP address, which is made up of a network identifier and a host identifier. The SG-DRL3-IP can only use Static IPs, DHCP is not supported. These options specify 4 bytes of the receiver IP address, from the high byte to low byte with highest (byte 3) in section [01] and lowest (byte 0) in section [04] in hexadecimal.

Defaults: 01: C0, 02: A8, 03: 00, 04: 01
(Represents: 192.168.000.001)

Options [05] - [08]: Receiver Subnet Mask Address

A mask used to determine what subnet an IP address belongs to. The subnet is 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. These options specify 4 bytes of receiver subnet mask address, from the high byte to low byte with highest (byte 3) in section [05] and lowest (byte 0) in section [08] in hexadecimal.

Defaults: 05: FF, 06: FF, 07: 00, 08: 00
(Represents: 255.255.000.000)

Options [09] - [0C]: Receiver Gateway

This is the address of the Gateway through which the SG-DRL3-IP must communicate to reach the T-LINK transmitter. This address is applied to all T-LINK modules connected to the SG-DRL3-IP.

These options specify the 4 bytes of the receiver gateway, from high byte to low byte with the highest (byte 3) in section [09] and the lowest (byte 0) in section [0C].

Defaults: 09: 00, 0A: 00, 0B: 00, 0C: 00
(Represents: 000.000.000.000)

Options [0D] - [0E]: Alarm Port Number

Use this option to set the Alarm Port connection number for your receiver. While the default value will suffice in environments involving just one receiver, Option [0D][0E] can be used to differentiate receivers in a complex, multiple receiver environment. If this option is changed, IP communication modules connected to the SG-DRL3-IP must be programmed with the new receiver number. Communications connected to the receiver will send their signals to this port.

Defaults: 0D: 0B, 0E: F5
(Represents: 3061)

Option [0F]: Receiver Number

The receiver number is used for sending signals to the central station software. Refer to the manuals for any central station automation software being used to determine if there are any special requirements for this number. Also, ensure that there are no duplicate receiver numbers used.

Default: 01

Option [10]: Line Card Number

The Line Card Number provides a virtual identification code for each SG-DRL3-IP module. Hexadecimal numbers "01" to "FE" can be programmed in Option [01] to identify line cards.

Default: 01

Option [11]: Line Card Number Length

This option is used to determine how many digits from the line card number will be sent to the output. You also have the option of displaying the number in hex or decimal. Program this option with one of the following:

01 Sends only one hex digit to the printer or computer output (if you have a 2-digit line card number only the last digit will be sent to the output).

02 Sends 2 hex digit line card number to the output.

03 Send 3 hex digit line card number to the output (leading zeros will be inserted prior to the line card number).

✓ **0A Send 3-digit line card number in decimal; send 2-digit receiver number in decimal**

0D Send 3-digit line card number in decimal

Option [12]: Debug Output

The debug mode should only be used when required and disabled after use. Enabling the Debug option reduces the SG-DRL3-IP receiver's ability to monitor the T-LINK transmitters.

✓ **00 Disabled**

Options [13] - [14]: Transmitter Absent Debounce Time

The time, in seconds, for which a transmitter configured in supervised mode must be absent before a transmitter failure condition will be reported. Valid entries are 30-65535 seconds. Value entered in hex.

Default: 078 (120s)

NOTE: Transmitter Absent Time should not be less than 90 seconds. For ULC Installations Security Level 4, this option shall be programmed as 5A (90s), 4B (75s) for Security Level 5. For UL Installations, this option shall be programmed as B4 (180s).

For UL Listed products, the permitted setting is 05AH(90s).

Options [15] - [16]: Transmitter Restoral Time

This option determines the required time a transmitter must be present before it is registered in the Account Table and the transmitter restoral message is sent.

Transmitter Restore Time must be 30 seconds minimum.

Default: 003C (60s)

For UL Listed products, the permitted setting is 05AH(90s).

Option [19]: Transmitter Restoral Trouble Mask

This programmable mask enables or disables the reporting of the Transmitter restoral condition on the SG-DRL3-IP receiver. Setting the mask to 0 signifies the trouble will be reported; setting the mask to 1 signifies the trouble will not be reported.

✓ **00 Condition reported**

01 Condition not reported (masked)

For UL Listed products, the permitted setting is OFF.

Option [1A]: Transmitter Failure Trouble Mask

This programmable mask enables or disables the reporting of the Transmitter failure/absent condition on the SG-DRL3-IP receiver. Setting the mask to 0 signifies the trouble will be reported; setting the mask to 1 signifies the trouble will not be reported.

✓ **00 Condition reported**

01 Condition not reported (masked)

For UL Listed products, the permitted setting is OFF.

Option [1B]: Transmitter Swap Trouble Mask

This programmable mask enables or disables the reporting of the T-LINK transmitter swap condition on the SG-DRL3-IP receiver. Setting the mask to 0 signifies the trouble will be reported; setting the mask to 1 signifies the trouble will not be reported.

- ✓ 00 Condition reported
- 01 Condition not reported (masked)

For UL Listed products, the permitted setting is OFF.

Option [1C]: Transmitter Unencrypted Trouble Mask

This programmable mask enables or disables the reporting of the T-LINK transmitter sending an unencrypted event when the SG-DRL3-IP is expecting an encrypted event condition on the SG-DRL3-IP receiver. Setting the mask to 0 signifies the trouble will be reported; setting the mask to 1 signifies the trouble will not be reported.

- 00 Condition reported
- ✓ 01 Condition not reported (masked)

For UL Listed products, the permitted setting is OFF.

Option [1D]: Invalid Report Trouble Mask

This programmable mask enables or disables the reporting of the invalid report condition. SG-DRL3-IP determines that the signal received is invalid, bad checksum, encryption key miss-match. Setting the mask to 0 signifies the trouble will be reported; setting the mask to 1 signifies the trouble will not be reported.

- ✓ 00 Condition reported
- 01 Condition not reported (masked)

For UL Listed products, the permitted setting is OFF.

Option [1E]: Unknown Account Trouble Mask

This programmable mask enables or disables the reporting of an unknown account report condition when the SG-DRL3-IP received is from an invalid account (not in the account table). Setting the mask to 0 signifies the trouble will be reported; setting the mask to 1 signifies the trouble will not be reported.

- ✓ 00 Condition reported
- 01 Condition not reported (masked)

For UL Listed products, the permitted setting is OFF.

Option [1F]: Accounts Exceeded Trouble Mask

This programmable mask enables or disables the reporting if the account table limit is exceeded when a new account tries to connect to a SG-DRL3-IP that has a full account table. Setting the mask to 0 signifies the trouble will be reported; setting the mask to 1 signifies the trouble will not be reported.

- ✓ 00 Condition reported
- 01 Condition not reported (masked)

For UL Listed products, the permitted setting is OFF.

Option [20]: Transmitter Deleted Trouble Mask

This programmable mask enables or disables the reporting when a T-LINK transmitter account deleted from the table. Setting the mask to 0 signifies the trouble will be reported; setting the mask to 1 signifies the trouble will not be reported.

- ✓ 00 Condition reported
- 01 Condition not reported (masked)

Option [2A]: For Future Use**Option [2B]: Busy Out**

The line card will stop acknowledging transmitter events under specific trouble conditions if Option [27] is programmed with the following:

- ✓ 00 No time set from CPM3, a code corruption checksum error, or an internal buffer is in full condition
- 01 Line card is being downloaded
- 04 No time set from CPM3, a code corruption checksum error, line card is being downloaded, if internal buffer is full, or loss of communication with the CPM3
- 05 No time set from the CPM3, automation computer is absent, loss of CPM3, line card is being downloaded

NOTE: If this 01 is selected, the line card will overwrite the oldest alarm with a new alarm when the internal buffer is full.

For UL Listed products, the permitted setting is 00.

Option [2C]: Internal Messages RS-232

When this option is programmed as '00', the SG-DRL3-IP will output its internal messages in the following format:

SRRLLL[#AAAA Nxyy]

If it is programmed as '01' internal messages will be output as:

ORRLLL[#AAAA Nxyy]

S, 0 (zero) = Protocol number

RR = Receiver number

LLL = Line number

AAAA = Account code, always 0000

00 = Output for all internal signals is SRRL protocol

✓ 01 = Output for all internal signals is ORRL protocol

02 = Output signals in automation protocol SRRL

03 with leading space in the zone (DVACS only)

= Output signals in automation protocol ORRL with leading space in the zone (DVACS only)

Options [2D] to [39]: For Future Use**Options [3A]-[3B] Console Port**

These options set the 2 byte Console **Connection Port Number** with high byte in section [3A] and low byte in section [3B]. If this option is changed, the console connected to the SG-DRL3-IP must be programmed with the new port number.

Defaults: 3A: 0B, 3B: F8
(Represents: 3064)

Options [40] - [43] Console Password

This is the password for the Account Port communication. In order for the user to be able to retrieve/modify the account table of the receiver the application must have a password that matches this section. Applications that connect to this port are:

T-Link Console

SG-Receiver Consoles

Table Loader

DLS (downloading software)

Default: 40:0C 41:0A 42:0F 43:0E
(Represents: CAFE)

Options [44]: DNIS Replacement of RRLLL

When set to 00 the SG-DRL3-IP will output the RRLLL (Receiver number and line number)

When set to 01 the SG-DRL3-IP will output the DNIS received from a GS transmitter instead of the RRLLL

Default: [00]

Options [45] Invalid Report Counter

Option 45 is used for limiting the number of invalid report messages that are sent to the printer and computer on encryption keys mismatch.

The default setting will send an invalid report for every 25 Invalid report (19 hex). To have every Invalid report sent to the computer and printer set Option 45 to 00.

For example, option = 19 (default), then the invalid counter is set for 25 consecutive occurrences to print invalid report for each individual account in the table. If the account is not in the table, a generic counter common to all invalid accounts will follow that same option.

Option [46]: Account Digit Stripping

The option controls the output of the account number set from 1 to 9 digits for both T-Link transmitter and panel account code. If the option is set to '00' T-Link transmitter account code will be sent to the output as 10 digits and panel account code will be sent as received.

For example if option [46] is set to '0x07' the following will occur:

Transmitter	Output
1234567890	4567890
0000001234	0001234
0012345678	2345678
Panel	Output
567890	567890
7890	7890
00567890	0567890

If the option [46] is set to '00' the following will occur:

Transmitter	Output
1234567890	1234567890
0000001234	0000001234
Panel	Output
567890	567890
7890	7890
00567890	00567890

Default: [00]

Option [47]: SIM Number Output

This option is available with the GS transmitter. When enabled, the receiver will output the received SIM number to the printer and automation. The message will include the account number (up to 10 digits following Option 56) and the SIM number (21 digits). The automation software used with the receiver will need to support the (s) protocol via the Sur-Gard output format in order for this feature to work.

The automation output is as follows:

sRRLLAAAAAAAAAASSSSSSSSSSSSSSSSSSSSS

Where

S is the protocol identifier

RRLlL is the Receiver and Line number of the line card that received the event

A is the 10 digit account number

S is the SIM number of the transmitter that sent the event

Default: [00]

Glossary

Account	The portion of a signal which contains the information identifying the location or the owner of the alarm panel. Also referred to as account number, account code or account digits.
Acknowledgement (ACK)	A signal sent from the receiver to the panel indicating that data has been received. A positive acknowledgement (ACK) means data was received without any detected errors (see kiss-off). A negative acknowledgement (NAK) means data was received, but there were detected errors. An acknowledgement may be sent per packet or per alarm.
AHS	Automatic Handshake Selection. See ANI.
Alarm	A message transmitted from the panel to the receiver containing account, event, zone, user or other information. There may be one or more per call. An alarm may be repeated in the same call (if not successfully delivered in a previous attempt). An alarm will contain one or more packets. Packets can contain rounds or different information. Alarm transmission is initiated with a handshake and, if received correctly, acknowledged with a kiss-off.
ANI	Automatic Number Identification. Refers to the receiver feature which enables the line card to request the handshake to be used with a particular panel from the CPM. The CPM maintains a database of most recently used handshakes for all accounts connected to the receiver. Handshakes are stored along with the phone number of the associated alarm panel.
ASCII	America Standard Code for Information Interchange. A seven-bit alphanumeric code used extensively in data communications. Parity is often added to the seven-bit code for error detection.
Automation	The combination of software package and PC which connects to the receiver to receive alarm events. The automation can be connected either by direct serial connection or TCP.
Automation Message	The alarm information delivered by a receiver in a specified protocol to a central station computer or network. Also referred to as a computer message
Backplane	See BP3.
Block	A group of data that specifically makes up one of the elements of an alarm. For example: account block, event block, or alarm block. One packet could contain multiple blocks.
BP3	A motherboard-style PCB which acts as the backbone for a single shelf of a System III receiver. The BP3 contains sockets to which up to 12 DRL3s, 1 CPM3, 1 PSC3 and 2 DC/DC3s can be connected. Furthermore, 2 BP3s can be connected together to form a 2-shelf configuration for the System III receiver. The BP3 also contains connections for a parallel printer and 2 serial automation COM ports, as well as an Ethernet connection. Also referred to as a backplane.
Busy Out	A state of a line card. Under predefined criteria the line card will go off-hook so as to not process any new alarms.
Call	The process of a receiver going off-hook, receiving one or more alarms and returning on-hook.
Caller ID	An FSK format received by the line card. This format can be received prior to sending the handshakes. The Caller ID data can be used by the receiver to provide additional information to all alarms received during a call.
Capture	The ability of a receiver to store commands sent to the panel from the automation computer after all of the alarms have been sent from the panel to the receiver.
Centronics	A parallel printer interface standard. Also known as standard IEEE1284. A centronics interface is implemented on the CPM3 (through the backplane) to interface to the local parallel printer.
Checksum	Additional data added to an alarm indicating whether the contents have been received correctly. This is generally done by summing all the digits in the message (mod 256) and reporting this as the checksum. Different methods of calculating a checksum may be specified in particular formats or protocols.
C.L.A.S.S	Custom Local Area Signaling Services. This term is used in the telephone industry to represent all features of a telephone line, such as Caller-ID, Call Forwarding, 3-Way Calling etc.
Client	One side of a two-sided TCP socket connection. The client is the one responsible for initiating the socket connection with the remote host (the server). The console represents the client side of the socket connection with the CPM3.
Computer Message	See Automation Message.
Console	A PC application program which can connect to the receiver and provide diagnostic/programming abilities to the user. For the System III, the console connects to the CPM3 via TCP/IP.
CPM3	Central Processing Module 3. The CPM3 controls the overall operation of the System III receiver, which includes multiplexing alarm signals from the line cards and sending them to the appropriate outputs
DC/DC3	The DC power supply of the System III receiver.
Dialer	Another name for a control panel.
DNIS	Dialed Number Identification Service.

DRL3	Digital Receiver Line Card 3.
DTMF	Dual Tone Multiple Frequency. A method of dialing which utilizes 2 sets of 4 tones (frequencies) each. Selecting one tone from each set will produce 16 distinct pairs. These pairs are used to dial digits when dialing a telephone number.
Equivalent Line Number	An option in the receiver. By default printer and computer messages will contain the line card number. Sometimes it is necessary to output the printer and computer messages with a different line card number; in this case this option can be used to overwrite the line card number in the printer and computer outputs of the receiver.
Event	The specific type of alarm being reported by the panel.
Event Code	A term used to describe a character or group of characters in an automation output. This character(s) is used to represent the event that was reported by the panel. Example 1: SG automation reports an alarm event using an event code of 'A', Restore as 'R', or Trouble as 'T'. Example 2: Sur-Gard automation reports using a SIA output for a burglary alarm an event code of 'BA'.
FES	Format Expert Systems. The name given to a receiver task which performs the basic functions of: 1. Sending handshakes; 2. Detecting the format from the panel; 3. Processing the alarm from the panel; 4. Sending a kiss-off to the panel.
Format	The pre-established order of events and meanings of the various characters in an alarm transmitted from a panel to a receiver.
FSK	Frequency Shift Keying. A modulation technique used with low-speed modems (300 to 1800 bps). The carrier frequency is shifted between two discrete frequencies in accordance with the binary serial data.
GSM	Global System for Mobile communications. Standard used for mobile phone.
Handshake	A signal sent by the receiver to a panel indicating that a connection has been established. These are either tones or modem data.
Heartbeat	A periodic signal sent from the automation outputter tasks to the automation software to verify the presence of that output. The period of this heartbeat is controlled via an option in the CPM3. Alternatively, the heartbeat refers to the signal sent between CPM3s to verify the presence/absence of each other.
Hook Flash	The process of the receiver going temporarily off-hook, usually in an attempt to transfer the phone call.
Hot-Swappable	Refers to the ability to add or remove particular cards to or from the system without removing power. In the System III, the CPM3, DRL3, DC/DC3 and PSC3 are all fully hot-swappable.
HTTP	Hypertext Transfer Protocol. A higher level protocol within the TCP/IP suite of protocols which is responsible for implementing web browsers. This is the protocol implemented by the CPM3 to enable the web interface to function.
IEEE 1284	See Centronics.
IEEE 802.3	See Ethernet.
Inter-burst Time	A term for the reception of pulse formats. The time between two bursts.
Inter-digit Time	A term used for reception of pulse or DTMF formats. The time between two digits.
Internal Trouble	A trouble condition which is generated inside a receiver, as opposed to being sent as an alarm from the panel. Internal troubles are also sent to the printer and automation outputs.
Kiss-off	A term used in the security industry for a positive acknowledgement.
Line	An individual channel on a line card. Equivalent to 1 telephone line.
Line Card	A removable, hot-swappable card which contains a POTS line interface which controls 1 or more POTS lines. For System III, each line card (DRL3) will interface to 1 line.
Line Conditioning	Electrical compensation for attenuation and phase delay distortion exhibited by the PSTN. Conditioning is performed through the use of an equalizer.
MAC Address	Media Access Control. A globally unique device 6-byte address which identifies a device attached to an Ethernet network. Assignment of MAC addresses is governed by the IEEE; any OEM company which manufactures Ethernet devices must apply for and purchase an OUI (Organizationally Unique Identifier), which consists of a block of 16,777,216 MAC addresses, all of which have the same first 3 bytes. Subsequent allocation of addresses within that block is at the discretion of the purchaser. Each Ethernet device produced must be programmed with a different MAC address in order to guarantee that each device will function correctly on the network. For the System III, the MAC address is stored in serial EEPROM on the CPM3 board. It is only programmable during manufacturing.
MLRF3	The metal rack which is used to enclose all other modules within a single shelf of the System III receiver.
MPC860	The Power PC microprocessor used as the main processor on the CPM3 board.

Multidrop	A communication link in which a single channel is shared by several stations or nodes (DVACS is a Multidrop network). Only one station may transmit at a time. Multidrop is also referred to as multipoint.
Negative Acknowledgement (NAK)	See acknowledgement.
Off-Hook	The process of connecting to the telephone line to answer an incoming call or dial a remote device (answering).
On-Hook	The process of releasing the telephone line after completion of a call (hanging up).
Options	A set of user-configurable parameters which controls the operation of a device. In the System III, both the DRL3 and the CPM3 contain sets of options. Static options affect all Profiles on a card. Dynamic options are unique to each profile.
Packet	A group of digits or characters of information in an alarm.
Panel	A device (the alarm system) at the protected premises used to transmit alarms to the receiver.
Ping	A standard network command which can be used to verify the presence of a device on a network, using the device IP address. Ping is implemented as part of the ICMP protocol and consists of the Echo Request and Echo Reply commands (poll and response respectively).
POTS	Plain Old Telephone System. An acronym used to describe a standard analog telephone network, or alternatively a standard analog telephone line.
Printer Message	The alarm information delivered by a receiver to a central station printer. This information is generally encapsulated in a descriptive English text message.
Profile	Generally refers to a group of options. The receiver can select a "profile" based on certain conditions.
Protocol	The pre-established order of events and meanings of the various characters in the information transmitted from a receiver to a monitoring computer.
PSC3	Power Supply Controller 3.
PSTN	Public Switched Telephone Network. Analogous to POTS.
PSU3	Power Supply Unit 3.
Receiver	The equipment used to receive alarms sent from panels. Sur-Gard's receivers are the SLR and the MLR. 'Receiver' is sometimes used interchangeably with 'line card' as it is the line card which actually receives the alarm in the MLR.
Ring	One of the wires used on a phone line, by convention this is red.
Rounds	Two or more packets of alarm information used for error checking. If two packets (rounds) are identical the packet contains valid data.
RRLLL	The part of the automation message which stores the receiver number and line card number. The length of this field is variable and is controlled via an option in both the line card and the CPM3.
Server	One side of a two-sided TCP socket connection. The server is the one responsible for receiving the socket connection with the remote host (the client). In general, a host which acts as a server can receive multiple client socket connection requests simultaneously. The CPM3 acts as a server to both the console and the web interface.
SG	Sur-Gard, a brand name of DSC. Also used to describe a particular type of automation output.
SIA	Security Industry Association. Sometimes referred to as the SIA format which is an example of FSK modulation.
RS-232	An asynchronous, point-to-point serial communications protocol. Used to communicate between the DRL3 and a PC for the DRL3's debug output. Also used to communicate between the CPM3 and the automation computer, and the CPM3 and a PC for the CPM3's debug output.
System III	Name given to a single entire receiver configuration, including rack, CPM3(s), line card(s), power supply, etc.
TCP/IP	Transmission Control Protocol/Internet Protocol. A standard network communications protocol. On the System III, TCP/IP is used to communicate between the console and the CPM3. It is also used to connect the CPM3 to a TCP printer (resident on the console) and TCP automation software (runs independent of the console).
Tip	One of the wires used on a phone line, by convention this is green.
UIB3	User Interface Board 3. An L-shaped board which connects to the CPM3 and contains output LEDs and 4 push buttons used for the user interface. This board also connects directly to the LCD screen.
Zone	The portion of an alarm which contains the information identifying the specific zone of the panel that has been violated.

Appendix A - CPM3 Internal Status Messages

Please refer to the System III Installation Manual.

Appendix B - DVACS Events

DVACS Generated Events

DVACS events generated on DVACS panels connected through the T-LINK TL250/TL300 will follow the same protocols used on the SG-DVL2A product.

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 -01-1-456--Fire Alm Zn999

Computer:

3011 456FA 999

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

Printer:

01 Nov 2004-13:51:03-01/02-SG -01-001-456--Medical Alm Zn001

Computer:

301001 456MA 001

Additional Events:

In the case of the T-LINK TL250/TL300 transmitter not receiving 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 001YC 000

Printer:

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

Computer:

3011 001YK 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).

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
- CPM3 Options [10] & [11] = 03

Appendix D - DEC-HEX-BIN Conversion Chart

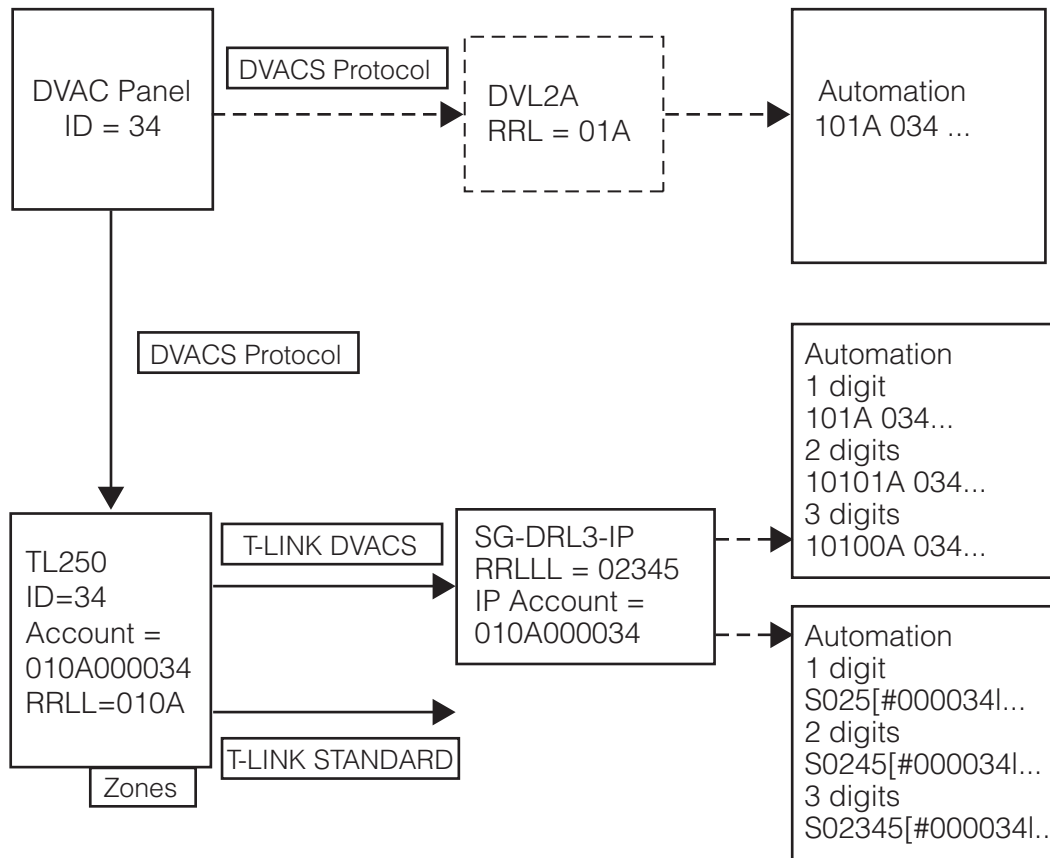
Dec	Hex	Binary	Dec	Hex	Binary
000	00	0000 0000	027	1B	0001 1011
001	01	0000 0001	028	1C	0001 1100
002	02	0000 0010	029	1D	0001 1101
003	03	0000 0011	030	1E	0001 1110
004	04	0000 0100	031	1F	0001 1111
005	05	0000 0101	032	20	0010 0000
006	06	0000 0110	033	21	0010 0001
007	07	0000 0111	034	22	0010 0010
008	08	0000 1000	035	23	0010 0011
009	09	0000 1001	036	24	0010 0100
010	0A	0000 1010	037	25	0010 0101
011	0B	0000 1011	038	26	0010 0110
012	0C	0000 1100	039	27	0010 0111
013	0D	0000 1101	040	28	0010 1000
014	0E	0000 1110	041	29	0010 1001
015	0F	0000 1111	042	2A	0001 1010
016	10	0001 0000	043	2B	0010 1011
017	11	0001 0001	044	2C	0010 1100
018	12	0001 0010	045	2D	0010 1101
019	13	0001 0011	046	2E	0010 1110
020	14	0001 0100	047	2F	0010 1111
021	15	0001 0101	048	30	0011 0000
022	16	0001 0110	049	31	0011 0001
023	17	0001 0111	050	32	0011 0010
024	18	0001 1000	051	33	0011 0011
025	19	0001 1001	052	34	0011 0100
026	1A	0001 1010	053	35	0011 0101

Appendix E - ASCII Character Chart

Corresponding ASCII on printer (Option 70) Hex Character

Code	Character	Code	Character	Code	Character
20	Space	43	I	50	P
30	0	44	J	51	Q
31	1	45	K	52	R
32	2	46	L	53	S
33	3	47	M	54	T
34	4	48	N	55	U
35	5	49	O	56	V
36	6	4A	C	57	W
37	7	4B	D	58	X
38	8	4C	E	59	Y
39	9	4D	F	5A	Z
41	A	4E	G	5C	\
42	B	4F	H		

Appendix F - DVACS Alarm Flow Comparison: SG-DVL2A Configuration / SG-DRL3-IP Configuration



Appendix G - T-LINK TL300 Contact ID Reports

On V1.20 or higher, the SG-DRL3-IP can receive Contact ID events from the T-LINK TL300. The Contact ID messages will be generated by the panel attached to the T-LINK TL300, including the panel

account code, please refer to the panel manufacturer documentation for all possible events for that panel. The T-LINK will still transmit its internal events in SIA.

Examples:

From panel through the T-LINK TL300:

12 Jul 2005 09:36:08 - 12 Jul 2005-09:36:06-01/03-SG -01-001-0092-E100-00 MEDICAL 000
 12 Jul 2005 09:36:11 - 12 Jul 2005-09:36:09-01/03-SG -01-001-0092-R100-00 MEDICAL 000

From the same T-LINK TL300 Input 3:

12 Jul 2005 09:37:20 - 12 Jul 2005-09:37:18-01/03-SG -01-001-0000001212--Nri1/FA0003
 12 Jul 2005 09:37:20 - 12 Jul 2005-09:37:18-01/03-SG -01-001-0000001212--Nri1/FH0003

FCC Compliance Statement

CAUTION: Changes or modifications not expressly approved by Digital Security Controls 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.

Important Information

This equipment complies with Part 68 of the FCC Rules and the requirements adopted by the ACTA. On the side of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the Telephone Company.

Product identifier: US:1VDAL03BSYSTEMIII

USOC Jack: RJ-21X

Telephone Connection Requirements

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

Ringer Equivalence Number (REN) The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local Telephone Company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format:

US: AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Incidence of Harm If this equipment Sur-Gard SYSTEM III causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the Telephone Company will notify the customer as soon as possible. Also,

you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

Changes in Telephone Company Equipment or Facilities The Telephone Company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the Telephone Company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

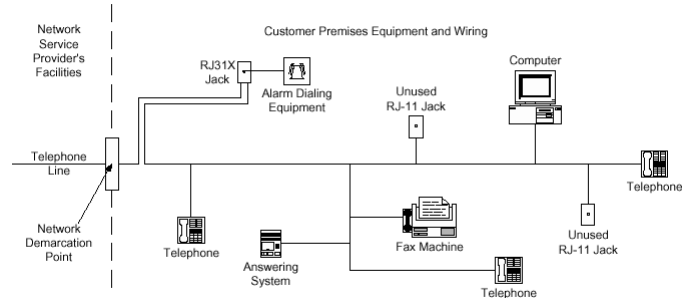
Equipment Maintenance Facility If trouble is experienced with this equipment Sur-Gard SYSTEM III, for repair or warranty information, please contact the facility indicated below. If the equipment is causing harm to the telephone network, the Telephone Company may request that you disconnect the equipment until the problem is solved. This equipment is of a type that is not intended to be repaired by the end user.

DSC c/o APL Logistics 757 Douglas Hill Rd. Lithia Springs, GA 30122

Additional Information

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Alarm dialing equipment must be able to seize the telephone line and place a call in an emergency situation. It must be able to do this even if other equipment (telephone, answering system, computer modem, etc.) already has the telephone line in use. To do so, alarm dialing equipment must be connected to a properly installed RJ31X jack that is electrically in series with and ahead of all other equipment attached to the same telephone line. Proper installation is depicted in the figure below. If you have any questions concerning these instructions, you should consult your telephone company or a qualified installer about installing the RJ31X jack and alarm dialing equipment for you.



Industry Canada Statement

IC: 160A-SYSTEM3

NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

DSC