TL280(R)

Internet Alarm Communicator - International

Installation Manual V4.1

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

Table of Contents

WARNING: Installer please read carefully

Note to Installers

The warnings on this page contain vital information. As the only individual in contact with system users, it is the installer's responsibility to bring each item in this warning to the attention of all 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 the reasons may be:

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.

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.

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.

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 the security system be reviewed periodically to ensure that its features remain effective and that it is updated or replaced if it is found that it does not provide the protection expected.

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.

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.

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.

Insufficient Time

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

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.

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.

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.

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.

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.

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, other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a hearing-impaired person.

General

IMPORTANT

This installation manual shall be used in conjunction with the control panel. All safety instructions specified within that manual shall be observed. The control panel is referenced as the "panel" throughout this document. This installation guide provides the basic wiring, programming and troubleshooting information. Use this guide in conjunction with the Installation Manual available online from the DSC website at www.dsc.com.

The Ethernet communicator is a fixed, wall-mounted unit, and shall be installed in the location specified in these instructions.The equipment enclosure must be fully assembled and closed, with all the necessary screws/tabs, and secured to a wall before operation. Internal wiring must be routed in a manner that prevents:

- Excessive strain on wire and on terminal connections,
- Interference between power limited and non power limited wiring,
- Loosening of terminal connections, or
- Damage of conductor insulation.

WARNING: Never install this equipment during a lightning storm!

Safety Information

The installer must instruct the system user on each of the following:

- Do not attempt to service this product. Opening or removing covers may expose the user to dangerous voltages or other risks.
- Any servicing shall be referred to service persons only.
- Use authorized accessories only with this equipment.
- Do not stay close to the equipment during device operation.

Model Information

This manual covers the following model of alarm communicator: TL280 and TL280R. References to model TL280(R) throughout this manual applies to all specified models unless stated differently. Models ending in "R" include a built-in RS-232 interface for connecting to local third party applications.

The TL280(R) is an Ethernet alarm communicator that sends alarm communication to Sur-Gard System I-IP, II, III (SG-DRL3IP), IV (SG-DRL4IP), and 5 (SG-DRL5IP) central station receivers through Ethernet/Internet.

The TL280(R) supports integration over IP and is available with licensed 3rd party product solutions. Specific programming for the related programming sections is to be provided by the 3rd party. A current list of compatible 3rd party solutions can be found at www.dsc.com.

The communicator can be used as either a backup or primary communicator. The communicator supports Internet Protocol (IP) transmission of panel and communicator events over Internet.

Panel Mounting

The TL280 communicator is compatible with HS2016, HS2032, HS2064, and HS2128 panels.

Features

- 128-bit AES encryption via Ethernet/Internet (NIST validation certificate number 2645).
- Ethernet LAN/WAN 10/100 BASE-T.
- Individual Internet periodic test transmission.
- Integrated call routing.
- Visual Verification (requires Sur-Gard System 5 Receiver)
- Remote firmware upgrade capability of the communicator and panel firmware via Internet.
- Panel remote uploading/downloading support via Internet.
- PC-LINK connection.
- SIA and Contact ID (CID) formats supported.
- Trouble display LEDs.
- Supervision heartbeats sent via Internet.
- Third party integration over cellular/IP. The product supports third party application via serial (R-models only) and Ethernet. Refer to third-party application documentation for more information.

EN50131-1 Installation Requirements

For EN50131-1 compliant installations, the following programming options shall be set as described.

Supervision Heartbeat (required for ATS4 and ATS5):

- **[851][004]** set to 0087h (135s heartbeat).

NOTE: The compatible receiver at ARC location shall have supervision window programmed for 1800s (ATS4) or 180s (ATS 5).

- **[851][005]** options 1 and 3 shall be enabled

Test transmission (required for ATS3):

- **[851]** System test options **[026]** and **[027]** shall be enabled (FF) for the communication paths available.
- **[851][124]** and **[125]** shall be programmed with time of day for test transmission and 1440 minutes (24h) for test transmission cycle

Configuration of communication paths (all ATS classes)

- **[300][001]** select option 02 for auto routing (this will allow transmission of the events over all available communication paths in the system)
- **[380]** enable option 5 (YES) for parallel transmission over all available communication paths (if redundant configuration is desired)
- **[382]** enable option 5 (YES) this will enable Alternate communicator
- **[384]** enable the desired back-up configuration (receiver 2 back-up for receiver 1 or receiver 3 back-up for receiver 1).

Technical Specifications, Ratings and Compatibility

Table 1: Communicator Ratings

Model	TL280(R)
Power Supply Ratings	
Input Voltage	10.8-12.5 VDC. Power is supplied from the panel's PC-Link header or a PCL-422 module in remote cabinet installations. In remote cabinet installations, the PCL-422 module located with the communicator is powered by either an HSM2204 or an HSM2300. Refer to the PCL-422 installation instructions for details.
Current Consumption	
Current	100mA @ 13.66V
Environmental Specifications	
Operating Temperature	-10°C to 55°C
Humidity	5% ~ 93% relative humidity, non-condensing
Mechanical Specifications	
Board Dimensions (mm)	100 × 150 × 15
Weight (grams) with bracket	290

Table 2: Compatible Receivers and Panels

Communicator	Receiver/Panel	Description
3G2080(R)	Receiver	• Sur-Gard System I-IP Receiver, version 1.13+ • Sur-Gard System II Receiver, version 2.10+ • Sur-Gard SG-DRL3-IP, version 2.30+ (for Sur-Gard System III Receiver) • Sur-Gard SG-DRL4-IP version 1.20+ (for Sur-Gard System IV Receiver) • Sur-Gard SG-DRL5-IP version 1.00+ (for Sur-Gard System 5 Receiver)
TL2803G(R)	Panel	• HS2016 • HS2032 • HS2064 • HS2128

NOTE: Enter [*][8][Installer Code][900] at keypad to view the panel version number.

Pre Installation Configuration

Encryption

The communicator uses 128 Bit AES encryption. Encryption can only be enabled from the monitoring station receiver. Each receiver (Ethernet 1 and 2) can independently have encryption enabled or disabled. When encryption is enabled, the central station will configure the device to encrypt communications the next time the communicator module performs a communication to that receiver.

NOTE: Packets will start being encrypted only after the next event is sent to that receiver, or if the unit is restarted.

Communicator Installation Configuration

This Ethernet communicator shall be installed by service persons only (service person is defined as a person having the appropriate technical training and experience necessary to be aware of hazards to which that person may be exposed to in performing a task and can also take measures to minimize the risks to that person or other persons). The Communicator shall be installed and used within an environment that provides the pollution degree max 2, overvoltages category II, in non-hazardous, indoor locations only. This manual shall be used with the installation manual of the panel which is connected to the communicator. All instructions specified within the panel manual must be observed.
All the local rules imposed by local electrical codes shall be observed and respected during installation.

Installing the Ethernet Cable

A Category 5 (CAT 5) Ethernet cable must be run from a source with Internet connectivity to the communicator module, inside the panel. The communicator end of the cable must be terminated with an RJ45 plug, which will connect to the communicator's RJ45 jack after the communicator is installed. All requirements for installation of CAT5 Ethernet cable must be observed for correct operation of the communicator, including, but not limited to, the following:

- Do NOT strip off cable sheathing more than required for proper termination.
- Do NOT kink/knot cable.
- Do NOT crush cable with cable ties.
- Do NOT untwist CAT5 pairs more than ½ in. (1.2cm).
- Do NOT splice cable.
- Do NOT bend cable at right angles or make any other sharp bends.

NOTE: CAT5 specification requires that any cable bend must have a minimum 2 in. (5 cm) bend radius. Maximum length of CAT 5 cable is 328 ft. (100 m).

Running the RS-232 Cable (R models only)

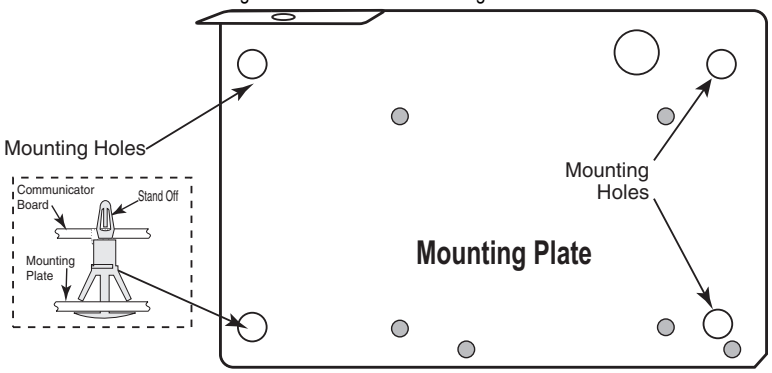
When installing the communicator for use with 3rd party applications an RS-232 cable must be connected between the 3rd party device and the communicator module.
NOTE: Maximum cable length for RS-232 cable is 8 ft. (2.4 m).
Please refer to the installation manual for the 3rd party device for wiring instructions.

Installing Communicator in Panel

Installing Communicator with HS2016, HS2032, HS2064, and HS2128 Panel

1. To assemble supplied mounting bracket, perform the following: (See **Figure 1**).
   a. Remove the 4 white plastic standoffs from the bag provided with the communicator kit.
   b. Insert the 4 standoffs through the back of the mounting bracket, into the holes at each corner.
   c. Place the bracket on a flat, solid surface. Hold the communicator component side up and orient the 4 holes on the communicator with the 4 standoffs protruding from the bracket. Push the communicator firmly and evenly onto the standoffs until it is securely attached to the mounting bracket.
   d. Remove the panel front cover.
   e. Remove and discard the circular knockout located in the top-right section of the panel.

Figure 1: Communicator Mounting Bracket

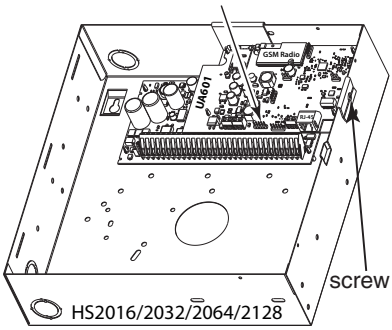


2. Install the Communicator into the panel:
   a. Attach one end of the PC-LINK cable to the panel PCLINK_2 header on the panel (red wire goes on the right-hand pin of the **panel** PCLINK_2 header (see **Figure 3**)).
   b. Insert the assembled communicator into the panel.

c. Locate the screw hole on the right side wall of the panel. See **Figure 2** "screw". Line up the assembled communicator with the right side wall of the panel and, using the screw provided, secure the mounting bracket to the panel.

d. Attach the other end of the PC-LINK cable to the communicator (red wire goes on the right-hand pin of the **communicator** PC-LINK header (See **Figure 3**)).

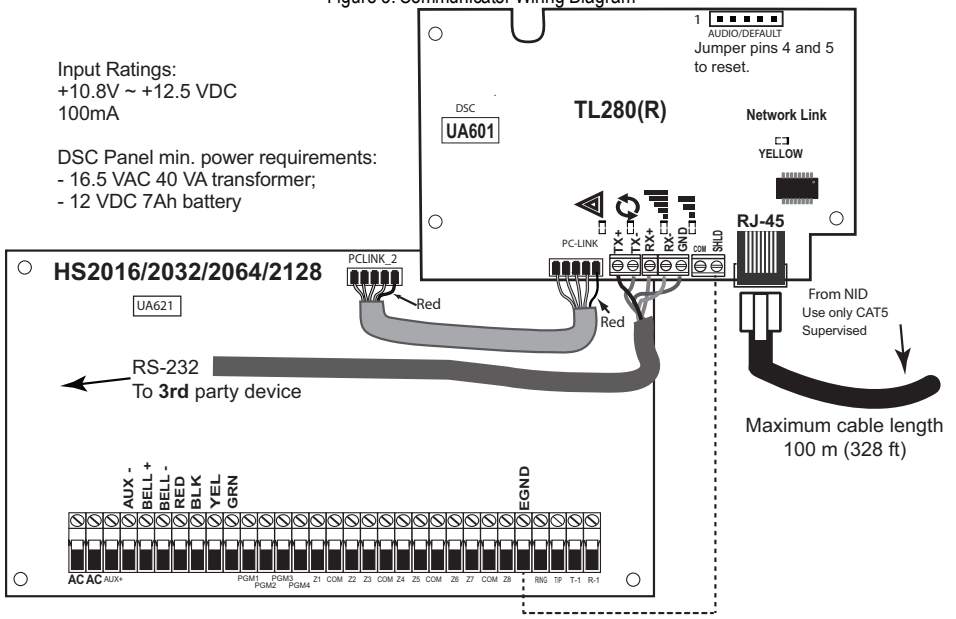
Figure 2: HS2016/2032/2064/2128 Control Panel



WARNING! - Modules are power limited. Do not route any wiring over the circuit board. Maintain at least 1in. (25.4mm) separation between circuit board and wiring. A minimum of ¼ in. (7mm) separation must be maintained at all points between non-power limited wiring and power limited wiring.

3. To electrically connect the communicator to the panel, perform the following steps (See **Figure 3**).
   a. Disconnect both AC power and battery connections from the panel, and disconnect telephone line.

Figure 3: Communicator Wiring Diagram



4. Install the RS-232 connections (R models only). If using the communicator with a 3rd party device, wire the connections as per the table below. Maximum cable length for RS-232 cable is 8 ft. (2.4 m).

NOTE: Please refer to the installation manual for the 3rd party device for wiring instructions.

Table 3: RS-232 Connections

3rd Party Device	Communicator
TX	RX+
Unused	RX-
RX	TX+
Unused	TX-
GND	GND

Install Network Cable

1. Route the CAT 5 Ethernet cable through back of the panel and plug it into the communicator's RJ45 jack.
2. Perform the following steps for initial power on of the panel with communicator installed:
   a. Reconnect the AC power, telephone line, and battery + connector to the panel. (The communicator and panel will power up together).
   b. Observe that the communicator's red and yellow LEDs are flashing together while it initializes. The red and yellow LEDs will continue to flash until the communicator has successfully communicated to all programmed receivers. If this is the first time the communicator has been powered up, the module will not be able to initiate communication until it has been programmed.

NOTE: Initialization may take several minutes to complete. Red and yellow LEDs will flash together during initialization. Do not continue to next step until the red and yellow LEDs have stopped flashing. (If only the yellow LED is flashing, there is a communicator trouble). Correct trouble indicated by flashes on yellow LED before continuing. (for troubleshooting assistance see Table 6).

3. Mount the panel in location.

Initial Panel Programming

Keypad Data Display

NOTE: Programming locations are accessible via the keypad.

- **Section-Toggle Options:** The number is displayed when toggle is ON, the number is not displayed when toggle is OFF. (e.g., toggle options displays: [--3--6--]. Options 3 and 6 are ON, all others are OFF). Pressing keys 1 through 8 will alternately turn the toggle ON and OFF.
- **HEX/Decimal Data:** Values that are provided with two defaults, separated by a "/" character, use the format: hexadecimal followed by decimal equivalent (e.g., default [0BF5/3061]). Hexadecimal numbers are shown, with all leading zeros, to the full field length defined for the number.

Entering HEX values at keypad

To enter HEX values at the keypad, press the * key before entering the HEX value. (e.g., to enter "C" at the keypad, press [*][3])

Entering ASCII Characters at keypad

1. Press [*] and use scroll buttons [<] [>] to display "ASCII Entry" on the LCD screen.
2. Press [*] to select ASCII entry mode.
3. Use the [<] [>] scroll keys to display the desired character and press [*] to save and exit ASCII.
4. Repeat the steps above to enter another ASCII character.

HS2016/2032/2064/2128 Initial Programming

Please refer to the panel manual for details. Perform the following steps to ensure that the communicator and the panel work together as intended. These sections must be programmed at the panel keypad. Enter [*][8][Installer Code][Section Number]. Record any values that are modified from their default, in the appropriate worksheets for the panel or communicator.

1. In panel section **[377]** 'Communication Variables', subsection **[002]** 'Communication Delays', sub-subsection **[1]** 'Communication Delay', program **060** (seconds).
2. In panel section **[382]** 'Communicator Option 3' set option **[5]** ON.

NOTE: If this option is OFF, the yellow status LED on the communicator will indicate 'Panel Supervision Trouble' (2 flashes) and the unit can not be programmed via the PC-LINK cable.

NOTE: Account number in communicator section **[851][021]** automatically syncs with panel system account number in section **[310][000]** 'Account Code'.

3. In panel sections **[300]** subsections **[001]** to **[004]**, program the subsection with **02** to **06**.

Table 4: Communicator Path Programming

Value	Communication Method
02	Auto Routing
03	Ethernet 1
04	Ethernet 2

NOTE: Refer to panel manual for additional information

4. In panel section [**350**] 'Communication Formats', program the communication format as: CID (03) or SIA FSK (04).
5. In panel sections [**311**] - [**318**] 'Partition Call Directions', program the call direction options for the system.
6. In panel section [**401**] 'DLS/SA Options', set toggle option [**2**] 'User Enable DLS' to ON in order to perform panel DLS session through cellular or Ethernet.

NOTE: Before leaving the premises, the installer should verify all programmed communications paths. See programming options section [**851**][**901**] to send immediate test transmissions.

Communicator Troubles displayed on a HS2016/2032/2064/2128

The communication trouble is the only trouble that will appear on the keypad Liquid Crystal Display (LCD) when encountered by a communicator installed in a HS2016/2032/2064/2128. For more information about the trouble on the communicator module refer to the panel event buffer or by accessing *2 to view the individual trouble types. Log entry will show Fault or Restore for each of the following events:

- Alt comm SIM lock Trouble/Restore
- Alt. comm Cellular Trouble/Restore
- Alt. comm Ethernet Trouble/Restore
- Alt. comm Fault/Restore
- Alt comm Receiver (1-4) Absent/Restore
- Alt comm Receiver (1-4) Supervision Trouble/Restore
- Alt comm Receiver (1-4) FTC Trouble/Restore

NOTE: When Panel displays "Alternate Fault", communicator programming is not accessible via the keypad.

Communicator Status LEDs

The communicator has 2 on-board LED indicators: a yellow trouble LED and a red network connection status LED.

⚠ Yellow Trouble LED

This yellow LED will flash to indicate a trouble on the unit. The number of flashes indicates the type of trouble. See the table below for the coded flashes and the conditions which will activate the trouble status LED.

Table 5: Yellow Trouble Status LED

# of Flashes	Trouble	# of Flashes	Trouble
2	Panel Supervision Trouble	8	Receiver Supervision Trouble
4	Not Applicable	9	FTC Trouble
5	Not Applicable	10	Not Applicable
6	Ethernet Trouble	12	Module Configuration Trouble
7	Receiver Not Available Trouble		

NOTE: Only the highest priority trouble (2 flashes is the highest priority trouble) is indicated. When this trouble is restored, the next highest trouble will indicate, if present. This will continue until all troubles have been cleared (yellow LED is not flashing).

The following paragraphs describe the conditions associated with the trouble indicated:

Panel Supervision Trouble (2 Flashes)

This trouble will be indicated when communication between the communicator module and the panel fails. If the module can not communicate with the panel (e.g., loss of power to the panel) the communicator will send the 'Panel Absent Trouble Event' message to the central station receiver. When communication returns, a 'Panel Absent Restore Event' is sent by the communicator to the central station receiver. The reporting codes are ET0001 for trouble and ER0001 for restore. The panel absent event always uses the primary receiver account code when communicating to the central station.

NOTE: The panel supervision trouble/restore are internally generated events by the communicator. Trouble is generated if the communicator misses 6 polls. Trouble is restored on receipt of first poll from the panel.

Ethernet Trouble (6 Flashes)

This trouble is indicated when Ethernet link between the transmitter and the local switch or router is absent. This trouble will also be indicated if the unit fails to get Dynamic Host Control Protocol (DHCP) settings from the DHCP server. (Not active if Ethernet receivers are not programmed).

Receiver Not Available (7 Flashes)

This trouble is indicated if the unit is not able to successfully initialize with any of the programmed receivers. Unprogrammed receivers are excluded.

Receiver Supervision Trouble (8 Flashes)

This trouble is indicated when receiver supervision is enabled and communication between the communicator module and the receiver fails. Trouble is indicated if Ethernet 1 is supervised and does not receive a heartbeat from the receiver.

FTC Trouble (9 Flashes)

This trouble is indicated when the unit fails to communicate module events to the central station. Trouble is displayed after the unit has exhausted all communications attempts to all programmed receivers for events generated by the communicator.

Module Configuration Trouble (12 Flashes)

This trouble is indicated when the system account code or the receiver account have not been programmed. Disabled receivers are excluded.

⚠ Red Network Connection Status LED

BLINKING: Indicates communications in progress.

- Once quickly for outgoing Ethernet transmission.
- Twice quickly to indicate incoming Ethernet ACK/NACK.

OFF: This is the normal state of the red network connection status LED. There are no network connection issues present.

ON: There is a problem with the Ethernet or the cellular network connection. LED will be ON if any of the following occur:

- Ethernet cable is not connected
- DHCP configuration times out.

Network Activity LED (Red)

- **Ethernet Activity**: Red LED will blink quickly once for transmit, or twice for receive.

Communicator Troubleshooting

NOTE: For additional details:

- Refer to section [983] for troubleshooting the firmware updates
- Refer to section [984] to verify the trouble status

Table 6: Trouble Indications

Trouble Indication	Trouble Indicator Digit	Possible Causes	Trouble Possible Solution
No Indication	N/A	No Power	• Check the power connections between the panel and the communicator. • Confirm PC-LINK cable is properly installed between communicator and panel.
Yellow LED – 2 Flashes	02	Panel Supervision Trouble	• Check section [382] toggle option[5] is ON (Alternate Communicator Enabled). • Ensure the PC-LINK cable between the panel and communicator is connected properly (not reversed) and is securely in place.
Yellow LED – 6 Flashes	06	Ethernet Trouble	• Check with the ISP to confirm Internet service is active in the area. • Ensure the Ethernet cable is securely inserted into the RJ45 jack of the communicator and the hub/router/switch. • Check the link light on the hub/router/switch is ON. If link light is OFF, start the hub/router/switch. • If DHCP is used, ensure that the unit has an assigned IP address from the server. In Section [851] [992] verify a valid IP address is programmed. If not, contact the network administrator. • If problem persists, replace the Ethernet cable and RJ45 connector.

Trouble Indication	Trouble Indicator Digit	Possible Causes	Trouble Possible Solution
Yellow LED – 7 Flashes	07	Receiver Not Available	• Ensure that the Ethernet path has Internet connectivity. • If using a static IP address, confirm that the gateway and subnet mask are entered correctly. • If the network has a firewall, ensure the network has the programmed • outgoing ports open (default UDP port 3060 and port 3065). • Ensure that all the receivers are programmed for DHCP or have the proper IP address and port number.
Yellow LED – 8 Flashes	08	Receiver Supervision Trouble	• This trouble is indicated when supervision is enabled and the unit is not able to successfully communicate with the receiver. • If this trouble persists, contact the central station.
Yellow LED - 9 Flashes	09	FTC Trouble	• The unit has exhausted all communications attempts to all programmed receivers for events generated by the communicator. • Restart the system, if trouble persists, contact the dealer.
Yellow LED – 12 Flashes	0C	Module Configuration Trouble	• This indication appears when section [021] system account code or sections [101] or [111] receiver account code have not been programmed. Ensure that a valid account code has been entered in these sections.
Red and Yellow LEDs flashing together	N/A	Initialization Sequence	• The unit is still initializing please wait while the unit gets its programming and establishes a connection to all programmed receivers. **NOTE: This process may take several minutes to complete.**
		Boot Loader Failed	• If the initialization sequence is taking more than several minutes, the boot loader might have failed. • Confirm that the boot loader has failed by entering communicator programming [*][8][installer code][851]. • If access is granted, continue waiting for the initialization sequence to complete. • If access is denied (long error tone), disconnect power from, then reconnect power to the communicator module.

.

Ethernet Programming Options

The programming sections described in this document can be viewed at the keypad LCD. To start programming enter: [*][8] [installer code][851][section number], where section number is the 3-digit section number referenced in this section. The programming worksheets at the end of this document can be used to record the new values when programming changes have been made from the default values.
Programming sections are accessed through the panel keypad. Installers may **set/review/record** programming options at the panel keypad.

System Options

[001] Ethernet IP Address

Default (000.000.000.000)
Enter the IP address of the communicator. Ensure that the IP address is unique to the communicator on the local network. Format is 4 fields, each field is a 3 digit decimal number. Valid range: 000-255. If an IP address is programmed in this section, the unit will operate with static IP (DHCP disabled). Sections [002] and [003] must also be programmed when using static IP addresses.
NOTE: Default for this section is Dynamic Host Configuration Protocol (DHCP) enabled. When enabled, the DHCP server will set values for: IP address [001], subnet mask [002], and gateway [003]. Programming an IP address in this section will disable DHCP (Static IP).

[002] Ethernet IP Subnet Mask

Default (255.255.255.000)
Enter the Ethernet IP subnet mask of the communicator. Format is 4 fields, each field is 3 digits. Valid range: 000-255.
NOTE: If DHCP is enabled, the DHCP server will assign the subnet mask for this section and the programmed value will be ignored.

[003] Ethernet Gateway IP Address

Default (000.000.000.000)

Enter the Ethernet gateway IP address of the communicator. The gateway IP address is required when a router is used on the local network to reach the destination IP address specified in section [001]. Format is 4 fields, each field is a 3 digit decimal number. Valid range: 000-255.

NOTE: If DHCP is enabled, the DHCP server will assign the gateway IP address for this section and the programmed value will be ignored.

[004] Receiver Supervision Interval

Default (0087/135)

When receiver supervision is enabled (ON) in section [005] toggle option [3], the unit sends heartbeats to Ethernet receiver 1 to test the communications path. Use this section to set the interval time (in seconds) when heartbeats will be sent to the receiver. Valid range 000A-FFFF seconds. If the programmed value is less than (000A/10) seconds, supervision is disabled.

- **Receiver Window:** This is the supervision timeout that must be configured at the central station receiver.
- **Recommended Values:** This is the recommended heartbeat interval that should be programmed into the communicator.

[005] System Toggle Options

[1] Ethernet Receiver 1 Supervised Default (OFF)

ON: Ethernet receiver 1 will be supervised and heartbeats will be sent to Ethernet receiver 1 based on the supervision interval programmed in section [004].

OFF: Ethernet receiver 1 will not be supervised. When disabled, heartbeat 1 is sent to the Ethernet receiver once every hour, regardless of supervision type (heartbeat 1 or 2). The heartbeat is resent every 5 seconds until ACK. If no event or heartbeat ACK is received after (receiver supervision interval + 75 seconds), supervisory trouble is indicated.

NOTE: Ethernet receiver 2 can not be supervised.

[2] Reserved

[3] Supervision Type Default (OFF)

ON: Heartbeat 1 (commercial supervision). This supervision type is suitable for applications where swap detection is required on the supervisory packet.

OFF: Heartbeat 2 (residential supervision). This supervision type is suitable for applications where supervision of the communication path to the receiver is required. (no swap detection).

NOTE: Commercial supervision is more data intensive than residential supervision and should only be used when required to meet the approval for the installation.

[4]-[5] Reserved

[6] Remote Firmware Upgrade Default (ON)

ON: The communicator module firmware can be remotely upgraded using the Ethernet.

OFF: The communicator module firmware can not be remotely upgraded. Local firmware upgrade is still possible.

[7] Alternate Test Transmissions Default (OFF).

ON: When the periodic test transmission interval occurs, the test transmission will alternate between being sent to the primary and secondary receivers with each test transmission interval.

OFF: When the periodic test transmission interval occurs, the test transmission will be sent to the programmed receivers, based on the settings of the periodic test transmission reporting codes.

[8] Reserved

[006] System Toggle Options 2

[1] Ethernet 1 receiver enabled. Default (ON).

ON: Ethernet receiver 1 is enabled.

OFF: Ethernet receiver 1 is disabled.

[2] Ethernet receiver 2 is enabled. Default (ON).

ON: Ethernet receiver 2 is enabled.

OFF: Ethernet receiver 2 is disabled.

[3]-[7] Reserved

[8] Network Trouble Suppression. Default (OFF).

ON: GSM/Ethernet/Supervisory troubles follow a delay timer as programmed in section [226].

OFF: GSM/Ethernet/Supervisory troubles are not suppressed.

[007] DNS Server IP 1

Default (000.000.000.000)

Enter the IP address for DNS server 1. Format is 4 fields, each field is a 3-digit decimal. Valid range: 000-255.

NOTE: If no value is programmed and DHCP is used, the DHCP server will configure the address. If an address is programmed and DHCP is used, the programmed address will be used instead of the DHCP address.

[008] DNS Server IP 2

Default (000.000.000.000)

Enter the IP address for DNS server 2. Format is 4 fields, each field is a 3-digit decimal. Valid range: 000-255.

NOTE: If no value is programmed and DHCP is used, the DHCP server will assign this value. If an address is programmed and DHCP is used, the programmed address will be used instead of the DHCP address.

Programming Options

[010] System Toggle Options 3

[1] Reserved.

[2] Visual verification. Default (OFF)

ON: Visual verification is enabled.

OFF: Visual verification is disabled.

[3]-[8] Reserved.

[011] Installer Code

Default (CAFE)

Program the installer code for the communicator module. The installer code will be required when programming the communicator module. Valid range: 0000 - FFFF.

[012] DLS Incoming Port

Default (0BF6/3062)

The DLS incoming local port (listening port) is the port DLS V will use when connecting to the communicator. If a router or gateway is used, it must be programmed with a transmission control protocol (TCP) port forward for this port to the communicator module IP address. Valid range: 0000 - FFFF.

[013] DLS Outgoing Port

Default (0BFA/3066)

The DLS outgoing port is used for outgoing session to DLS V after an SMS request has been sent to the communicator. Use this section to set the value of the local outgoing port. The value must be changed if the communicator is located behind a firewall and must be assigned a particular port number, as determined by the network administrator. In most cases, changing the default value or configuring the firewall with this port is not required.

Valid range: 0000-FFFF.

NOTE: If section [006] toggle option [7] is ON, DLS will use the primary path for session. If section [006] toggle option [7] is OFF DLS will use the Ethernet path, if available.

[015] DLS Call-Up IP

Default (000.000.000.000)

[016] DLS Call-Up Port

Default (0000)

[020] Time Zone

Default (00)

Please refer to panel manual section 'Real Time Clock' for more details. Use Column 2 (Offset Hours) to find the local Time Zone. Record the two digit HEX value from Column 1 (HEX Value) on the same row. Program this HEX value for the Time Zone. Valid range is 00 - FF.

Table 7: World Wide Time Zones

HEX Value	Offset Hours	Standard Abbreviation	Location
01	-12	BIT	Baker Island Time
05	-11	SST	Somoa Standard Time
09	-10	HAST	Hawaii-Aleutian Standard Time
0B	-9.5	MIT	Marquesas Island Time
0D	-9	AKST	Alaska Standard Time
11	-8	PST	Pacific Standard Time
15	-7	MST	Mountain Standard Time
19	-6	CST	Central Standard Time
1D	-5	EST	Eastern Standard Time
1F	-4.5	VST	Venezuela Standard Time
21	-4	AST	Atlantic Standard Time
23	-3.5	NST	Newfoundland Standard Time

HEX Value	Offset Hours	Standard Abbreviation	Location
25	-3	ART	Argentina Time
29	-2	BEST	Brazil Eastern Standard Time
2D	-1	CVT	Cape Verde Time
31	0	GMT	Greenwich Mean Time (UTC)
35	1	CET	Central European Time
39	2	SAST	South Africa Standard Time
3D	3	AST	Arabic Standard Time
3F	3.5	IRST	Iran Standard Time
41	4	GST	Gulf Standard Time
43	4.5	AFT	Afghanistan Time
45	5	PKT	Pakistan Time
47	5.5	IST	Indian Standard Time
48	5.75	NPT	Nepal Time
49	6	VOST	Vostok Time
4B	6.5	MMT	Myanmar Time
4D	7	BDT	Bangladesh Standard Time
51	8	CST	China Standard Time
52	8.25	APO	Apo Island Time
54	8.75	ACWST	Australian Central Western Standard Time
55	9	KST	Korea Standard Time
57	9.5	ACST	Australian Central Standard Time
59	10	AEST	Australian Eastern Standard Time
5B	10.5	LHST	Lord Howe Standard Time
5D	11	VUT	Vanuatu Time
5F	11.5	NFT	Norfolk Island Time
61	12	NZST	New Zealand Standard Time
64	12.75	CHAST	Chatham Island Standard Time
65	13	TOT	Tonga Time
69	14	LINT	Line Island Time
70-FF	N/A	N/A	N/A

[021] Account Code

Default (FFFFFF)

The account code is included when transmitting any events generated by the communicator. (e.g., panel absent trouble). It is recommended that the account code be the same as the control panel account number. Valid range: 000001-FFFFFE. If 4 digit account codes are needed the 2 lowest digits must be programmed as FF (e.g., Account 1234 is programmed as:1234FF).

NOTE: Programming this section with all 0 or F will cause a module configuration trouble.

NOTE: This section shall sync with panel option [310] with PowerSeries Neo Panels version 1.00 or higher.

[022] Communications Format

Default (04)

Program 03 for Contact ID (CID). Program 04 for SIA. The module can be configured to send Events in SIA or CID format. The SIA communication format follows the level 2 specifications of the SIA Digital Communication Standard - October 1997. This format will send the account code along with its data transmission. The transmission will look similar to the following at the receiver.

NOTE: This section shall sync with PowerSeries Neo panels version 1.00 or higher.

Example:

Nri0 ET001 where: **N** = New Event; **ri0** = Partition/Area identifier; **ET** = Panel Absent Trouble; **001** = Zone 001.

Communications Reporting Codes

Table 8: Communications Reporting Codes

Event	SIA Identifier	SIA ReportingCode	CID Qualifier	CID Event Code	CID Reporting Code	CID User/Zone
[023] Panel Absent Trouble	ET	0001	1	3	55	001
[024] Panel Absent Trouble Restore	ER	0001	3	3	55	001
[026] Ethernet 1 Test Transmission	RP	0001	1	6	A3	951
[027] Ethernet 2 Test Transmission	RP	0002	1	6	A3	952
[030] FTC Restore	YK	0001	3	3	54	001

[023] Panel Absent Trouble

Default (FF)
Program 00 to disable this event or FF to enable. This event will occur when communications with the panel have been lost for more than 60 seconds.

[024] Panel Absent Trouble Restore

Default (FF)
Program 00 to disable this event or FF to enable. This event will occur when communications with the control panel have resumed.

System Test Options

Test Transmissions to Primary Receiver, with Backup to Secondary Receiver:

Set Ethernet section [026] to (FF); [027] to (00).

- If the test transmission fails to the primary receiver it will backup to the secondary receiver.
- If the test transmission fails to the secondary receiver an FTC trouble will be generated.

Independent Test Transmission to Primary and Secondary Receivers:

Set Ethernet section [026] to (FF); [027] to (FF).

- The module will send periodic test transmissions to each receiver independently, with no backups.
- If the test transmission fails to any of the programmed receivers, an FTC trouble will be generated.

Alternating Test Transmission:

Alternate test transmission can be enabled or disabled in section [005] toggle option [7].

Alternating Test Transmission with backup receivers:

Set Ethernet section [026] to (FF); [027] to (00).
Interval 1:

- If the test transmission fails to the primary receiver it will backup to the secondary receiver.
- If the test transmission fails to the secondary receiver an FTC trouble will be generated.

Interval 2:

- If the test transmission fails to the secondary receiver it will backup to the primary receiver.
- If the test transmission fails to the primary receiver an FTC trouble will be generated.

Test Transmission Unique to Primary and Secondary Receivers:

Set Ethernet section [026] to (FF); [027] to (FF).
Interval 1:

- The module will send periodic test transmissions to primary receivers (Ethernet primary) independently, with no backups.
- If the test transmission fails to any of the programmed primary receivers, an FTC trouble will be generated.

Interval 2:

- The module will send periodic test transmissions to secondary receivers (Ethernet secondary) independently, with no backups.
- If the test transmission fails to any of the programmed secondary receivers, an FTC trouble will be generated.

[026] Ethernet 1 Transmission

Default (FF)
Program 00 to disable this event transmission or FF to enable. See system test options (above) for details on settings.

[027] Ethernet 2 Transmission

Default (00)
Program 00 to disable this event transmission or FF to enable. See system test options (above) for details on settings.

[030] FTC Restore

Default (FF)

Program 00 to disable this event transmission or FF to enable. This event will occur when an FTC Trouble on the system restores.

[037] System Firmware Update Fail

Default (FF);

Program 00 to disable this event transmission or FF to enable. This event will occur when the panel firmware updated has failed.

Table 9: System Firmware Update Fail

Event	SIA Identifier	SIA ReportingCode	CID Qualifier	CID Event Code	CID Reporting Code	CID User/Zone
[037] System FW Update Fail	LU	0000	1	9	04	003

NOTE: The communicator will report ´System Update Fail´ only if the panel becomes offline after a remote firmware update session has started.

[095] SA Incoming Local Port

Default (0000)

[096] SA Outgoing Local Port

Default (0000)

[097] SA Call Up IP

Default (000.000.000.000)

[098] SA Call Up Port

Default (0000)

[099] SA Access Code

Default (FFFFFFFF)

Ethernet Receiver 1 Options

[101] Ethernet Receiver 1 Account Code

Default (0000000000)

The account code is used by the central station to distinguish between transmitters. This account code is used when transmitting heartbeat signals to the central station receiver. Signals received from the panel will use the control panel account number. Valid range: 0000000001-FFFFFFFFFE. Programming all 0 or all F will cause a module configuration trouble.

[102] Ethernet Receiver 1 DNIS

Default (000000)

The Dialed Number Information Service (DNIS) is used in addition to the account code to identify the communicator module at the central station. Valid range: 000000 - 099999. Value is entered as a leading 0 followed by the 5 digit DNIS. Format is Binary Coded Decimal (BCD).

NOTE: Each Ethernet receiver must be programmed with a unique DNIS.

[103] Ethernet Receiver 1 Address

Default (127.000.000.001)

The default address enables the communicator to operate in Unattended Mode.

Unattended mode is used when a receiver is not available and the unit is required to perform DLS sessions. Typically used where the customer programs the control panel daily due to access control and still wants to receive alarms without buying extra hardware (receiver) or software.

NOTE: When a valid IP address has been programmed, Ethernet receiver 1 is enabled and will communicate events over the Ethernet channel.

[104] Ethernet Receiver 1 UDP Remote Port

Default (0BF5/3061)

This section determines the UDP remote port of Ethernet receiver 1. Valid range: 0000 - FFFF.

[105] Ethernet Receiver 1 UDP Local Port

Default (0BF4/3060)

Use this section to set the value of the UDP local outgoing port. Set the value of this port when the installation is located behind a firewall and must be assigned a particular port number as determined by the central station system administrator. Valid range: 0000 - FFFF.

[106] Ethernet Receiver 1 Domain Name

Default ( ) Enter the domain name as 32 ASCII characters.

Ethernet Receiver 2 Options

[111] Ethernet Receiver 2 Account Code

Default (0000000000)

The account code is used by the central station to distinguish between transmitters. The account code is used when transmitting heartbeat signals to the central station receiver. Signals received from the control panel will use the control panel account number. Valid range: 0000000001- FFFFFFFFFE. Programming all 0 or all F will cause a module configuration trouble (yellow LED=12 flashes).

[112] Ethernet Receiver 2 DNIS

Default (000000)

The DNIS is used in addition to the account code to identify the communicator module at the central station. Valid range: 000000 - 099999. Value is entered as leading 0 followed by the 5-digit DNIS. Format is BCD.

NOTE: Each Ethernet receiver must be programmed with a unique DNIS.

[113] Ethernet Receiver 2 Address

Default (000.000.000.000)

Programming the Ethernet receiver 2 IP address with 000.000.000.000 will disable Ethernet.

Enter the Ethernet receiver 2 IP address. This address will be provided by the central station system administrator. Format is 4 fields, each field is a 3-digit decimal. Valid range: 000-255.

NOTE: When a valid IP address has been programmed, Ethernet receiver 2 is enabled and will communicate events over the Ethernet channel.

NOTE: Do not program Ethernet receivers 1 and 2 to communicate to the same receiver.

[114] Ethernet Receiver 2 UDP Remote Port

Default (0BF5/3061)

This section is used to program the port number used by Ethernet receiver 2. Set the value of this port when the installation is located behind a firewall, and must be assigned a particular port number as determined by the central station system administrator. Valid range: 0000 - FFFF.

NOTE: Do not program Ethernet receiver 1 and Ethernet receiver 2 port with the same value.

[115] Ethernet Receiver 2 UDP Local Port

Default (0BF9/3065)

Use this section to program the value of the local outgoing port. Set the value of this port when the installation is located behind a firewall and must be assigned a particular port number as determined by the network administrator. Valid range: 0000 - FFFF.

NOTE: Do not program Ethernet receiver 1 and Ethernet receiver 2 port with the same value.

[116] Ethernet Receiver 2 Domain Name

Default ( ) Enter the Domain Name as 32 character ASCII.

Ethernet Options

[124] Ethernet Test Transmission Time

Default (9999)

Enter a 4 digit number (0000-2359) using the 24-hour clock format (HHMM) to set the test transmission time of day. Valid range: 00 - 23 hours (HH) and 00 - 59 minutes (MM). Programming a value of 9999 will disable the test transmission time.

NOTE: The internal date and time will automatically be programmed when the unit communicates with the primary receiver.

[125] Ethernet Test Transmission Cycle

Default (000000)

This value represents the interval between test transmissions, in minutes. Valid range: 000000 - 999999 minutes. Once the unit has sent the initial periodic test transmission, all future test transmissions will be offset by the programmed number of minutes. See sections [026] - [027].

Table 10: Ethernet Test Transmission Interval

Test Transmission Interval	Daily	Weekly	Monthly
Programmed Minutes	001440	010080	043200

NOTE: Minimum value is 000005 minutes. Programming an interval that is less than 5 minutes will disable test transmission.

[226] Network Trouble Delay

Default (0F)

This option is used to program the delay, in minutes, for reporting/displaying a network trouble. Valid entries are 00 - FF (e.g., for a 10 minute network trouble delay enter: 0A). When this Timer is programmed as 00, Ethernet and Supervision troubles are not communicated or displayed on the keypad.

[651] Integration Account Code

This section will display the unique 12-digit number assigned to this communicator for the identification when integrated with third party applications.

[652] Integration Access code

This section is a programmable 8 digit number used for initialization with third party applications.

[663] Integration Toggle Option 2

This toggle options in this section are used to enable and configure the path used for integration with third party applications.

NOTE: Only one integration path can be enabled at a time .

[1] Integration Over Serial Toggle Default (ON)

ON: Integration over serial enabled.

OFF: Integration over serial disabled.

[2] Reserved.

[3] Integration Over Ethernet Toggle Default (OFF)

ON: Integration over Ethernet enabled.

OFF: Integration over Ethernet disabled.

[4] Reserved.

[5] Integration Protocol Default (ON)

ON: Integration protocol enabled.

OFF: Integration protocol disabled.

[6]-[8] Reserved

[664] Integration Toggle Option 3

The toggle options in this section are used to determine the polling and notification behavior used for integration with third party applications.

[1] UDP Polling Default (OFF)

[2] TCP Polling Default (OFF)

[3] Real-time Notification Default (OFF)

[4] Notification Follows Poll Default (OFF)

[5]-[8] Reserved.

[665] Integration Polling Interval in Seconds

(Default: 000A)

This option controls the polling interval from the alarm panel to the integration interface for the purpose of optimizing data usage. The shorter the interval, the higher the data usage. Valid range: 0000-FFFF.

Receiver Diagnostic Testing

[693] Integration Server IP

This section displays the IP address of the third party server. **Do not** program this section if a domain name is programmed in setion [697].

[694] Integration Notification Port

This section is used to program the TCP Integration port for real time notification

[695] Integration Polling Port

This section is used to program the integration server port. Refer to third party device manual for more information

[697] Integration Server DNS

Enter the domain name (up to 32 ASCII characters) as provided by a third-party device. Refer to third party device manual for more information.

[698] Integration outgoing port

This section is used to program the outgoing port for integration via UDP.

[699]Integration incoming port

This section is used to program incoming port for integration via TCP.

[901] Diagnostic Test Transmission

[1] Ethernet 1 (OFF).

[2] Ethernet 2 (OFF).

[3] - [8] Reserved (OFF).

This section may be used by the installer to force the communicator to send an immediate test transmission to specific receivers, to verify that the communications paths are available. Diagnostic test transmission failure will indicate as FTC trouble (yellow LED = 9 flashes). If an FTC error occurs when testing all receivers, select only one receiver and repeat test to isolate the receiver that is not communicating.

NOTE: Sending a test transmission to a receiver that is not programmed generates FTC trouble.

System Information (Read Only)

NOTE: Sections [983] - [998] are provided for information (read only). Values in these sections cannot be modified by the installer.

[983] Firmware Update Diagnostics Section

Firmware updates for panel and the communicator itself can be made from the communicator.

- The firmware update diagnostic section is a read only 2-digit, hexadecimal section.

Table 11: Response Code Descriptions and Corresponding Actions

Response Code	Description of Response Code	Corresponding Action
Bad File		
00	Version check failed	Contact DSC Tech Support, described the action attempted with the system and supply them with the Response Code in Section [983].
01	Image type mismatch	
02	Device type mismatch	
03	Hardware type mismatch	
04	General variant mismatch	
05	Firmware header wrong length	
Panel is Busy		
20	System update pending - panel is armed	Disarm the panel to continue with system firmware update process.
21	System update pending -AC trouble (Any AC trouble; device/module)	Resolve the AC trouble to continue with system firmware update process.
22	System update pending -low battery (Any low battery trouble; device/module)	Resolve the low battery trouble to continue with system firmware update process.
25	System update pending - communication in progress	Retry in a few minutes; if issue persists, contact DSC Tech Support.
Firmware Update Sequence Change		
A0	System firmware update successful	None
A1	System firmware update failure	At least one module was not updated. Use DLS to reapply the firmware to the module not updated.
A2	System firmware update failure - module not found	At least one module was not responding during firmware update. Ensure all modules enrolled are physically connected and powered up.
AA	Device firmware transfer begin	None
AB	Device firmware module update begin	None
AC	General device firmware transfer failure	Contact DSC Tech Support, describe the action attempted with the system and supply them with the Response Code in Section [983].
Firmware Update Status		
C0	System ready to update.	None
C1	System update cancel request received	The system has received an update cancel request from DLS.
C2	System update begin	None
Firmware Download Request Reject		

Response Code	Description of Response Code	Corresponding Action
E0	Reserved	
E1		
E2		
E3		
E4		
E5	Remote firmware update disabled	Enable remote firmware update in the communicator in order to perform remote system firmware update.
Local Status Update States		
FE	Firmware file empty	No action required. Communicator currently does not have any firmware files.
FD	Firmware download in progress	No action required. Communicator is currently downloading firmware.

The table above displays the firmware update indicator codes and meaning of each code. The updates can be made from communicator. Communicator can update firmware of the panel and also of communicator itself. This section does not provide specific details such as if the image is still stored or erased due to the cancellation code.

[984] Communicator Status

The communicator status sections provide the installer with the status of the communicator's functionality, operational readiness, and failures.

The communicator status is displayed as a 6-digit hexadecimal code. The code ranges between 00000F and 2220CF, though not all numbers in this range are assigned. Each of the 6 digits represents a status or trouble indicator as below:

1. Digits 1 & 2: Reserved.
2. Digit 3: Network Indicator, indicates the operational status of the network.
3. Digits 4 & 5: Trouble Indicator displays the type of issue on the communicator or modules associated with and connected to communicator. See Table 6 on page 12 for a listing of possible values.
4. Digit 6: Reserved, displays as 'F' or '-'.

For example, a value of 11002F means:

11- Reserved.

0 - No network issues

02 - Panel supervision trouble with the communicator

The status code for the radio signal strength, its typical troubles, possible causes and troubleshooting instructions is displayed in the table below.

Table 12: Network Indicator - Digit 3

Network Indicator Value	Means
OFF	No network trouble
ON	Ethernet cable disconnected Ethernet DHCP failed
Flashing	Incoming transmission Outgoing transmission Incoming transmission

[987] Language Version

This section will display the current language version of the communicator.

[988] DNS 1 IP Address

This section will display the IP address of DNS Server 1. This is useful when the unit is configured for DHCP and the IP address was assigned to the device by the DHCP server is needed. This value is programmed in Section [007] or assigned by DHCP.

[989] DNS 2 IP Address

This section will display the IP address of DNS Server 2. This is useful when the unit is configured for DHCP and the IP address that was assigned to the device by the DHCP server is needed. This value is programmed in section [008] or assigned by DHCP.

[990] Boot Loader Version

This section will display the current boot loader version of the communicator.

[991] Firmware Version

This section will display the current firmware version of the device. Update worksheets with new version after a flash update is completed.

[992] Ethernet IP Address

This section will display the IP address of the Ethernet connection. This value is programmed in section [001] or assigned by DHCP.

[993] Ethernet Gateway Address

This section will display the IP address of the Ethernet gateway. This value is programmed in section [003] or assigned by DHCP.

[998] MAC Address

This section will display the unique12-digit, hexadecimal number assigned as the Media Access Control (MAC) address of the device.

System Reset Defaults

[999] Software Default

Default (99);
The software default allows the installer to refresh the unit after changes and also return the communicator to the default state.
00: Default Module. All programming sections in module revert to factory settings. This will erase all existing programming of the unit.
55: Reset. The communicator is reset. This option is equivalent to power cycling the communicator.

Ethernet Cellular Programming Worksheets

System Options

[001] Ethernet IP Address
Default (000.000.000.000)

[002] Ethernet IP Subnet Mask
Default (255.255.255.000)

[003] Ethernet Gateway IP Address
Default (000.000.000.000)

[004] Receiver Supervision Interval
Default (0087/135) Valid range: 0000 - FFFF.

[005] System Toggle Options

- [1] Ethernet Receiver 1 Supervised Default (OFF).
- [2] Reserved.
- [3] Supervision Type Default (OFF).
- [4] Reserved.
- [5] Reserved.
- [6] Remote Firmware Upgrade Default (ON).
- [7] Alternate Test Transmission Default (OFF).
- [8] Reserved.

[006] System Toggle Options 2

- [1] Ethernet Receiver 1 Enabled Default (ON).
- [2] Ethernet Receiver 2 Enabled Default (ON).
- [8] Network Trouble Suppression Default (OFF).

[007] DNS Server IP 1
Default (000.000.000.000)

[008] DNS Server IP 2
Default (000.000.000.000)

Programming Options

[010] System Toggle Options 3

- [1] Reserved
- [2] Visual Verification Default (OFF).
- [3] Reserved

[011] Installer Code
Default (CAFE) Valid range: 0000 - FFFF.

[012] DLS Incoming Port
Default (0BF6/3062) Valid range: 0000 - FFFF.

[013] DLS Outgoing Port
Default (0BFA/3066) Valid range: 0000 - FFFF.

[015] DLS Call-Up IP
Default (000.000.000.000)

[016] DLS Call-Up Port
Default (0000) Valid range: 0000 - FFFF.

[020] Time Zone
Default (00) Valid range: 00 - 99.

[021] Account Code
Default (FFFFFF) Valid range: 000001 - FFFFFE.

[022] Communications Format
Default (04) Program 03 (CID), 04 (SIA).

[023] Panel Absent Trouble
Default (FF); Program 00 disable or FF enable.

[024] Panel Absent Trouble Restore
Default (FF) Program 00 disable or FF enable.

System Test Options

[026] Ethernet 1 Transmission
Default (FF) Program 00 disable or FF enable.

[027] Ethernet 2 Transmission
Default (00) Program 00 disable or FF enable.

[030] FTC Restore
Default (FF) Program 00 disable or FF enable.

[037] Panel Firmware Update Fail
Default (FF) Program 00 disable or FF enable.

[095] SA Incoming Local Port
Default (0000) Valid range: 0000 - FFFF.

[096] SA Outgoing Local Port
Default (0000) Valid range: 0000 - FFFF.

[097] SA Call Up IP
Default (000.000.000.000)

[098] SA Call Up Port
Default (0000) Valid range: 0000 - FFFF.

[099] SA Password
Default (FFFFFFFF) Valid range: 00000000 - FFFFFFFF.

Ethernet Receiver 1 Options

[101] Ethernet Receiver 1 Account Code
Default (0000000000)
Valid range: 0000000001 - FFFFFFFFFE.

[102] Ethernet Receiver 1 DNIS
Default (000000) Valid range: 000000 - FFFFFF.

[103] Ethernet Receiver 1 Address
Default (127.000.000.001)

[104] Ethernet Receiver 1 UDP Remote Port
Default (0BF5/3061) Valid range: 0000 - FFFF.

[105] Ethernet Receiver 1 UDP Local Port
Default (0BF4/3060)Valid range: 0000 - FFFF.

[106] Ethernet Receiver 1 Domain Name
Default ( ) 32 ASCII characters.

Ethernet Receiver 2 Options

[111] Ethernet Receiver 2 Account Code
Default (0000000000)
Valid range: 0000000001 - FFFFFFFFFE.

[112] Ethernet Receiver 2 DNIS
Default (000000) Valid range: 000000 - 0FFFFF.

[113] Ethernet Receiver 2 Address
Default (000.000.000.000)

[114] Ethernet Receiver 2 UDP Remote Port
Default (0BF5/3061) Valid range: 0000 - FFFF.

[115] Ethernet Receiver 2 UDP Local Port
Default (0BF9/3065) Valid range: 0000 -FFFF.

[116] Ethernet Receiver 2 Domain Name
Default ( )

Ethernet Options

[124] Ethernet Test Transmission Time
Default (9999) Valid: 00-23(HH); 00-59(MM)

[125] Ethernet Test Transmission Cycle
Default (000000)
Valid range: 000000 - 999999 minutes.

[226] Network Trouble Delay
Default (0F)
Valid entries from, 00 to FF.

[651] Integration Identification Number
Default ()

[652] Integration Access Code
Default ()

[663] Integration Toggle Options 2

- [1] Integration Over Serial Port (ON)
- [2] Reserved
- [3] Integration Over Ethernet (OFF)
- [4] Reserved
- [5] Integration Protocol (ON)
- [6] Reserved
- [7] Reserved
- [8] Reserved

[664] Integration Toggle Options 3

- [1] UDP Polling (OFF)
- [2] TCP Polling (OFF)
- [3] Real-time Notification (OFF)
- [4] Notification Follows Pool (OFF)
- [5] Reserved
- [6] Reserved
- [7] Reserved
- [8] Reserved

[665] Integrated Poll Interval in Seconds
Default (000A) Valid range: 0000 - FFFF.

[693] Integration Server IP
Default (000.000.000.000).

[694] Integration Notification Port

Default (0C00/0372) Valid range: 0000 - FFFF.

[695] Integration Polling Port

Default (0C01/3073) Valid range: 0000 - FFFF.

[697] Integration Server DNS

32 ASCII characters.

---

[698] Integration Outgoing Port

Default (0C04/3076) Valid range: 0000 - FFFF.

[699] Integration Incoming Port

Default (0BFF/3071) Valid range: 0000 - FFFF.

Receiver Diagnostic Testing

[901] Diagnostic Test Transmission

[1] Ethernet 1 Default (OFF).
[2] Ethernet 2 Default (OFF).

System Information (Read Only)

[983] Firmware Update Diagnostics Section

[984] Communicator Status

[987] Language Version

[988] DNS 1 IP Address

[989] DNS 2 IP Address

[990] Boot Loader Version

[991] Firmware Version

[992] Ethernet IP Address

[993] Ethernet Gateway Address

[998] MAC Address

System Reset Defaults

[999] Software Default

Default (99); Valid entries are 00 or 55

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'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 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.

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.

EULA

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:

Software Installation and Use - For each license You acquire, You may have only one copy of the SOFTWARE PRODUCT installed.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

LIMITED WARRANTY

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.

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.

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.

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 MOD8IFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE PRODUCT.

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.

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.

Regulatory Information

EN50131 Compliant installations

1. The TL280R, TL280 module is monitored by the control panel and it is programmed via the programming menu (* 8, section [851] in the control panel. The interface is connected to the PC-Link bus as shown in the diagram included in this manual.
2. The Ethernet port is protected against surge transients up to 2.5kV and it is immune to conducted and radiated RF fields with levels up to 10V/m as tested per EN50130-4 Standard.
3. The TL280R, TL280 module conforms with radiated emissions levels for Class B equipment as per standards EN61000-6-3/EN55022/CISPR22.
4. The TL280R, TL280 module uses AES128 encryption and heartbeat supervision for both the Ethernet communication path and it meets security levels S2 as per EN50136-2-1 (EN50131-1). It also uses authentication for each message exchanged with the compatible receiver equipment at ARC and it meets level I2 for information security.
5. The TL280R, TL280 module has only one communication path: Ethernet 10/100 Base T using Internet/Intranet network.

TL280 and TL280R have been certified by Telefication in accordance with EN50131-1 requirements for Grade 2, Class II and ATS Class 3,4,5.

Hereby, DSC, declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The complete R&TTE Declaration of Conformity can be found at http://www.dsc.com/listings_index.aspx

(CZE) DSC jako výrobce prohlašuje, že tento výrobek je v souladu se všemi relevantními požadavky směrnice 1999/5/EC.

(DAN) DSC erklærer herved at denne komponenten overholder alle viktige krav samt andre bestemmelser gitt i direktiv 1999/5/EC.

(DUT) Hierbij verklaart DSC dat dit toestel in overeenstemming is met de eisen en bepalingen van richtlijn 1999/5/EC.

(FIN) DSC vakuuttaa laitteen täyttävän direktiivin 1999/5/EC olennaiset vaatimukset.

(FRE) Par la présente, DSC déclare que ce dispositif est conforme aux exigences essentielles et autres stipulations pertinentes de la Directive 1999/5/EC.

(GER) Hierdurch erklärt DSC, daß dieses Gerät den erforderlichen Bedingungen und Vorrausetzungen der Richtlinie 1999/5/EC entspricht.

(GRE) Δία του παρόντος, η DSC, δηλώνει ότι αυτή η συσκευή είναι σύμφωνη με τις ουσιώδης απαιτήσεις και με όλες τις άλλες σχετικές αναφορές της Οδηγίας 1999/5/EC.

(ITA) Con la presente la Digital Security Controls dichiara che questo prodotto è conforme ai requisiti essenziali ed altre disposizioni rilevanti relative alla Direttiva 1999/05/CE.

(NOR) DSC erklærer at denne enheten er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

(POL) DSC oświadcza, że urządzenie jest w zgodności z zasadniczymi wymaganiami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/WE.

(POR) Por este meio, a DSC, declara que este equipamento está em conformidade com os requisitos essenciais e outras determinações relevantes da Directiva 1999/5/EC.

(SPA) Por la presente, DSC, declara que este equipo está en conformidad con los requisitos esenciales y otros requisitos relevantes de la Directiva 1999/5/EC.

(SWE) DSC bekräftar härmed att denna apparat uppfyller de väsentliga kraven och andra relevanta bestämmelser i Direktivet 1999/5/EC.

Tech Support: 1-800-387-3630 (Canada & U.S.) or 905-760-3000
www.dsc.com

DSC
From Tyco Security Products

29009103R002