TL280(R)

Internet Alarm Communicator - North America

INSTALLATION MANUAL V4.0

Warning: This manual contains information on limitations regarding product use and function and information on the limitations as to liability of the manufacturer.

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 your 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 manual. All the safety instructions specified within that manual shall be observed. The control panel is referenced as the "panel" throughout this document.

The Internet alarm 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 alarm communicator models: TL280 and TL280R. Models ending in "R" include a built-in RS-422 interface for connecting to local third party applications.

TL280(R): Is an Internet 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 an Internet connection.

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 an Internet connection.

Panel Mounting

The TL280(R) 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 (Not a UL feature) (Requires a 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 Internet.

Technical Specifications

The input voltage to the Communicator can be drawn from an Underwriters Laboratories/Underwriters Laboratories Canada (UL/ULC) listed control panel or compatible power supply module such as HSM2204 or HSM2300.

NOTE: Power supply must be Class 2, power limited.

UL/ULC Installation Requirements

NOTE: For equipment used at the protected premises and intended to facilitate IP communications (hubs, routers, NIDs, Digital Subscriber Line (DSL), cable modems), 24 hour back-up power is required. Where such cannot be facilitated, a secondary (back-up) communication channel is required.

Domain Name Service (DNS) programming is not permitted in UL/ULC listed systems.

Notes for using Private, Corporate, and High Speed Data Networks:

Network access and domain access policies shall be set to restrict unauthorized network access, and spoofing or Denial of Service (DoS) attacks. Select an Internet Service Provider (ISP) that has redundant servers/systems, back-up power, routers with firewalls enabled, and methods to identify and protect against DoS attacks (e.g., via spoofing).

Notes for using Public Switched Data Networks:

Communication channels shall be facilitated such that the communicator will restrict unauthorized access, which could otherwise compromise security. The communicator shall be located in a secured area.

- For ULC Residential Fire and Burglary applications the TL280(R) can be used as primary communication channel via either Ethernet or as a back-up in conjunction with the Digital Alarm Communicator Transmitter (DACT). Test transmission every 24 hours shall be enabled on each channel.
- For ULC Commercial Fire and Burglary applications the TL280(R) can be used as a passive communication module with the following security levels:
  - P1 (each channel is independent)
- The communicator can also be used as an active communication system with the security levels A1-A4 (each channel independent). For active line security systems AES128 bit encryption shall be enabled (at the monitoring station receiver) and the supervision heartbeat rate shall be set as 90 seconds (panel section [851][004] = 005A/90). The supervision window at the Signal Receiver Center (SRC)'s receiver shall be programmed as maximum of 180 (00B4/180) seconds.
- For UL Residential Fire and Burglary applications the TL280(R) can be used as the primary communication channel via Ethernet, or as a back-up in conjunction with the DACT (30 day test transmission is required on each channel).
- The supervision heartbeat shall be enabled (panel section [851][005] toggle option [1] (Ethernet) shall be ON), toggle option [3] (supervision type) shall be ON and the supervision heartbeat rate shall be selected as 135 (0087/135) seconds. Option [004] = 0087. The supervision window at the supervising station shall be maximum 200 (00C8/200) seconds. For encrypted line security systems the encryption AES128 bit shall be enabled at the monitoring station receiver.
- For UL Commercial Burglary installations, the TL280(R) is listed as a primary (sole) communication means (heartbeat must be enabled) or for supplementary (back-up) use in conjunction with a Plain Old Telephone Service (POTS) line dialer. When the heartbeat transmission over the Ethernet network is enabled, using the TL280(R) with a compatible control unit listed for standard/encrypted line security, it can provide line security for the alarm system over the primary line.
- The TL280(R) is also suitable for use with a compatible control unit listed for dual line security transmission when used in conjunction with a DACT or a Public Switched Data Network (PSDN) transmitter. The PSDN provides the line security and is the primary line. In this mode, alarm signals are required to be sent simultaneously over both communication methods.

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	14°F to 131°F (-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
TL280(R)	Receiver	• Sur-Gard System I 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)
	Panel	• HS2016 • HS2032 • HS2064 • HS2128

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

Products or components of products, which perform communications functions only, shall comply with the requirements applicable to communications equipment as specified in UL60950 or CAN CSA C22.2. No. 60950-1, Information Technology Equipment - Safety - Part 1: General Requirements. Where network interfaces are external to the control unit or receiver, compliance to CAN CSA C22.2. No. 60950-1 is adequate. Such components include, but are not limited to: hubs, routers, NIDs, third-party communications service providers, DSL modems, and cable modems.

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.

NOTE: Before leaving the installation site, the communicator TL280(R) Ethernet line shall be connected via an APPROVED (acceptable to the local authorities) Network Interface Device (NID) (e.g., for UL Installations, UL60950 listed NID). All wiring shall be performed according to the local electrical codes.

COMMUNICATOR INSTALLATION CONFIGURATION

The 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 Ethernet 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 Ethernet/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 CAT 5 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 CAT 5 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: CAT 5 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-422 Cable (R models only)

When installing the communicator for use with 3rd party applications an RS-422 cable must be connected between the 3rd party device and the communicator module.

NOTE: Maximum cable length for RS-422 cable is 1,000 ft. (305 m).

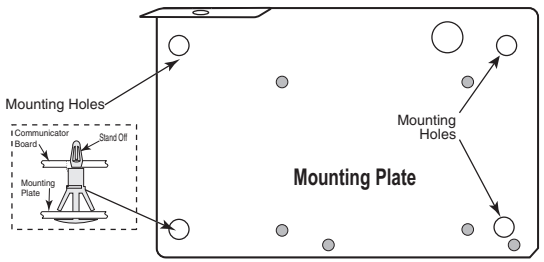
Please refer to the installation manual of the 3rd party device for wiring instructions.

INSTALLING ETHERNET 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



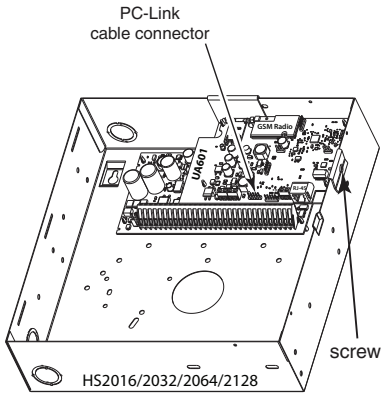
2. Install the Communicator into the panel:
   a. Attach one end of the PC-LINK cable to the PCLINK_2 header on the panel (red wire goes on the right-hand pin of the panel PCLINK_2 header (see Figure 3)).
   b. Insert the assembled communicator into the panel.

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)).

e. Using light pressure (finger tight only), attach the supplied white quad band whip antenna to the threaded antenna connection point at top of the panel.

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

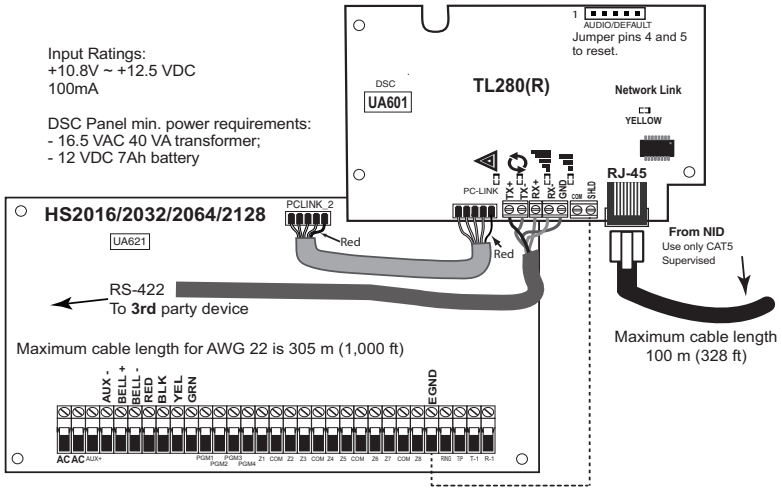


WARNING! - The TL280(R) module is power limited. Do not route any wiring over the circuit board. Maintain at least 1in. (25.4mm) separation between circuit board and wiring. A minimum of ¼ in. (7mm) separation must be maintained at all points between non-power limited wiring and power limited wiring.

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-422 connections (R models only). If using the communicator with a 3rd party device, wire the connections as per the table below:

Table 3: RS-422 Connections

3rd Party Device	Communicator
TX+	RX+
TX-	RX-
RX+	TX+
RX-	TX-
GND (Optional)	GND

NOTE: The GND connection is optional. DSC recommends connecting GND wire at both ends.

Install Network Cable

1. Route the CAT 5 Ethernet cable through back of the panel and plug it into the communicator's RJ45 jack.

NOTE: Before leaving the premises the Ethernet communication lines must first be connected to an approved (acceptable to local authorities) type NID, (UL installations, UL 60950 listed NID, for ULC installations CAN/CSA C22.2. No. 60950-1 certified NID). All wiring shall be performed according to the local electrical codes.

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.

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. (See Table 6 for troubleshooting assistance).

3. Mount the panel at location.

INITIAL PANEL PROGRAMMING

i **Domain Name Service (DNS) programming is not permitted in UL/ULC listed systems.**

Keypad Data Display

- 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 zeroes, to the full field length defined for the number.

Entering HEX values at keypad

To enter HEX values at the keypad, you must 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 character you want 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 installation guide section 'Alternate Communicator Set-up' 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].

3. In panel sections [300] 'Panel/Receiver Communications Paths' subsections [001] to [004], program the subsection with 02 to 04.

Table 4: Communicator Path Programming

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

NOTE: Refer to panel reference 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 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.

NOTE: Sending test transmissions to receivers that are not programmed will generate FTC Trouble.

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

If the The HS2016/2032/2064/2128 panel encounters a communicator trouble, a trouble message is displayed on the LCD keypad. For more information about the communicator trouble, press [*][2] or refer to the event buffer. The log entry shows Fault or Restore for each of the following events:

- Alt. Comm Ethernet Trouble/Restore
- Alt. Comm Fault/Restore
- Alt. Comm Receiver (1-2) Absent/Restore
- Alt. Comm Receiver (1-2) supervision Trouble/Restore
- Alt. Comm Receiver (1-2) 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. The LED meaning is described in this section.

⚠Yellow Trouble LED

The 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 is indicated. This will continue until all troubles have been cleared (yellow LED is not flashing).

The following paragraphs describe each trouble condition:

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: Panel supervision troubles/restores 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 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 RESET / UPDATE

Factory Defaults Reset

You can reset the programming options for the communicator to the factory settings by installing the hardware jumper. Perform the following steps to reset the communicator:

NOTE: A jumper is required on AUDIO/DEFAULT pins 4 and 5 to reset the hardware values.

1. Remove panel front cover.
2. Locate the AUDIO/DEFAULT 5 pin connector on the communicator board (see Figure 3).
3. Apply a jumper to short the hardware default pins 4 and 5.
4. Remove AC and DC power from the panel and then reapply power to the panel.
5. Wait 30 seconds.
6. Remove the jumper from the hardware default pins 4 and 5 (green LEDs will stop flashing).
7. Replace the panel cover.

NOTE: The communicator has now been reset to the factory default values.

Firmware Update

The device firmware can be updated over Ethernet (remote or local updating):

- When the firmware update begins, all LEDs are ON.
- During the firmware update process, the LEDs will cycle in a chaser pattern.
- During the firmware update process, the chaser pattern will briefly pause and resume again. This indicates firmware verification check has passed, and application update will begin.
- After a successful update, the unit will automatically restart.
- Should the update fail, all LEDs will flash ON, then OFF together at 1-second intervals.

NOTE: If the firmware update fails, restart the communicator by cycling power. For persistent update failures, contact your dealer. For UL/ULC listed installations, only local firmware updates are allowed.

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.
Trouble 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 your ISP to confirm Internet service is active in your area. • Ensure your 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.
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 your 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 your 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 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.

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 receivers. 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.
- For ULC installations, the daily test transmission must be enabled over each available communication channel sections [125].

Table 7: Supervision Intervals for UL/ULC

Jurisdiction	Receiver Window (Timeout)	Recommended Supervision Interval
UL Commercial Burglary	200 seconds	(0087/135) seconds
UL Residential Fire	30 days	Panel Test Transmission
UL Residential Burglary	30 days	Panel Test Transmission
ULC Commercial Burglary Active	180 seconds	(005A/90) seconds
ULC Commercial Burglary Passive	24 hours	Panel Test Transmission
ULC Commercial Burglary Fire Active	180 seconds	(0073/115) seconds
ULC Commercial Burglary Fire Passive	24 hours	Panel Test Transmission

[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.

OFF: Events will be communicated to the receivers individually.Toggle should be OFF when guaranteed message delivery to both receivers is required.

[4] Reserved

[5] Reserved

[6] Remote Firmware Upgrade Default (ON)

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

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]-[8] Reserved

[007] DNS Server IP 1

Default (000.000.000.000)

*Programming this section is **not** permitted on a UL/ULC listed system.*

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 address that you program will be used instead of the DHCP address.

[008] DNS Server IP 2

Programming this section is not permitted on a UL/ULC listed system.

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 address that you program 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] **Reserved**.
[4] **Reserved**.
[5] **Reserved**.
[6] **Reserved**.
[7] **Reserved**.
[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 IV 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 IV 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 your network administrator. In most cases, changing the default value or configuring your firewall with this port is not required.

Valid range: 0000-FFFF.

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

Table 8: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
01	-12	BIT	Baker Island Time
05	-11	NUT	Niue Time
		SST	Somoa Standard Time
09	-10	HAST	Hawaii-Aleutian Standard Time
		THAT	Tahiti Time
		TKT	Tokelau Time
		CKT	Cook Island Time
0B	-9.5	MIT	Marquesas Island Time
0D	-9	AKST	Alaska Standard Time
		GIT	Gambier Island Time
11	-8	PST	Pacific Standard Time
		PST	Pitcarirn Standard Time
		CIST	Clipperton Island Standard Time
15	-7	MST	Mountain Standard Time
19	-6	CST	Central Standard Time
		GALT	Galapagos Time
		PIT	Peter Island Time
		EAST	Easter Island Standard Time
1D	-5	EST	Eastern Standard Time
		COT	Colombia Time
		ECT	Ecuador Time
		PET	Peru Time
		ACT	Acre Time
1F	-4.5	VST	Venezuela Standard Time

Table 8: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
21	-4	AST	Atlantic Standard Time
		CLST	Chile Standard Time
		BWST	Brazil Western Standard Time
		SLT	San Luis Time
		PYT	Paraguay Time
		JFST	Juan Fernandez Island Standard Time
		GYT	Guyana Time
		FKST	Falkland Island Standard Time
		BOT	Bolivia Time
23	-3.5	NST	Newfoundland Standard Time
25	-3	CGT	Central Greenland Time
		ART	Argentina Time
		BRT	Brazilia Time
		UYT	Uruguay Standard Time
		SRT	Suriname Time
		ROTT	Rothera Time
		PMST	St. Pierre & Miquelon Standard Time
		GFT	French Guiana Time
29	-2	GST	South Georgia and the South Sandwich Islands
		BEST	Brazil Eastern Standard Time
2D	-1	EGT	Eastern Greenland Time
		CVT	Cape Verde Time
		AZOST	Azores Standard Time
31	0	WET	Western Europian Time
		GMT	Greenwich Mean Time (UTC)
		SLT	Sierra Leone Time
		IST	Ireland Standard Time
35	1	CET	Central Europian Time
		WAT	Western Africa Time
		BST	British Summer Time

Table 8: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
39	2	EET	Eastern Europian Time
		CAT	Central Africa Time
		SYT	Syrian Standard Time
		SAST	South Africa Standard Time
		IST	Israel Standard Time
3D	3	MSK	Moscow Standard Time
		EAT	Eastern Africa Time
		AST	Arabic Standard Time
		AST	Arabia Standard Time
		AST	Al Manamah Standard Time
3F	3.5	IRST	Iran Standard Time
41	4	AMST	Armenia Standard Time
		SCT	Seychelles Time
		GST	Gulf Standard Time
		SAMT	Samara Time
		RET	Reunion Time
		MUT	Mauritius Time
		ICT	Iles Crozet Time
		GET	Georgia Standard Time
		AZT	Azerbaijan Time
43	4.5	AFT	Afghanistan Time
45	5	WKST	West Kazakhstan Standard Time
		PKT	Pakistan Time
		YEKT	Yekaterinburg Time
		UZT	Uzbekistan Time
		TMT	Turkmenistan Time
		TJT	Tajikistan Time
		TFT	French Southern and Antarctic Time
		MVT	Maldives Time
		MAWT	Mawson Time
		KGT	Kyrgyzstan Time
		HMT	Heard and McDonald Island Time
		DAVT	Davis Time

Table 8: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
47	5.5	IST	Indian Standard Time
48	5.75	NPT	Nepal Time
49	6	XJT	Xinjiang Standard Time
		EKST	East Kazakhstan Standard Time
		LKT	Sri Lanka Time
		VOST	Vostok Time
		OMSK	Omsk Standard Time
		NOVT	Novosibirsk Time
		BTT	Bhutan Time
		BIOT	British Indian Ocean Time
4B	6.5	CCT	Cococ Islands Time
		MMT	Myanmar Time
4D	7	CXT	Christmas Island Time
		KOVT	Khovd Time
		KRAT	Krasnoyarsk Time
		WIB	Waktu Indonesia Bagian Barat
		ICT	Indochina Time
		BDT	Bangladesh Standard Time
51	8	AWST	Australian Western Standard Time
		CST	China Standard Time
		HKST	Hong Kong Standard Time
		WITA	Waktu Indonesia Bagian Tengah
		TWT	Taiwan Time
		SST	Scarborough Shoal Time
		SIT	Spratly Island Time
		SGT	Singapore Time
		PST	Philippine Standard Time
		PIT	Pratas Islands
		PIT	Parcel Island Time
		MYT	Malaysia Time
		MNT	Mongolia Time
		MBT	Macclesfield Bank Time
		ACIT	Ashmore and Cartier Island Time

Table 8: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
52	8.25	APO	Apo Island Time
54	8.75	ACWST	Australian Central Western Standard Time
55	9	YAKT	Yakutsk Time
		JST	Japan Standard Time
		KST	Korea Standard Time
		WIT	Waktu Indonesia Bagian Timur
		TPT	East Timor Time
		PWT	Palau Time
57	9.5	ACST	Australian Central Standard Time
59	10	AEST	Australian Eastern Standard Time
		GST	Guam Standard Time
		YAPT	Yap Time
		VLAT	Vladivostok Time
		TRUT	Truk Time
		PGT	Papua New Guinea Time
		DTAT	District de Terre Adelie Time
		ChST	Chamorro Standard Time
5B	10.5	LHST	Lord Howe Standard Time
5D	11	KOST	Kosare Standard Time
		NCT	New Caledonia Time
		VUT	Vanuatu Time
		SBT	Solomon Island Time
		PONT	Phonpei Standard Time
		MAGT	Magadan Island Time
5F	11.5	NFT	Norfolk Island Time

Table 8: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
61	12	NZST	New Zealand Standard Time
		FJT	Fiji Time
		WFT	Wallis and Futuna Time
		TVT	Tuvalu Time
		PETT	Petropavlovsk Time
		NRT	Nauru Time
		MHT	Marshall Island Time
		GILT	Gilbert Island Time
		ANAT	Anadyr Time
64	12.75	CHAST	Chatham Island Standard Time
65	13	PHOT	Phoenix Island Time
		TOT	Tonga Time
69	14	LINT	Line Island Time
70 - FF	N/A	Reserved	

[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 9: Communications Reporting Codes

Event	SIA Identifier	SIA Reporting Code	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 10: System Firmware Update Failure

Event	SIA Identifier	SIA Reporting Code	Contact ID Qualifier	Contact ID Event Code	Contact ID Reporting Code	Contact ID 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 your installation is located behind a firewall and must be assigned a particular port number as determined by your central station system administrator. Valid range: 0000 - FFFF.

[106] Ethernet Receiver 1 Domain Name

Default ( )

Enter the domain name as 32 ASCII characters.

Programming this section is not permitted on a UL/ULC listed system.

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: 000000000**1**-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 your 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 receiver 1 and Ethernet receiver 2 to communicate to 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 your installation is located behind a firewall, and must be assigned a particular port number as determined by your 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. You can set the value of this port when your installation is located behind a firewall and must be assigned a particular port number as determined by your 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 ( )

*Programming this section is **not** permitted on a UL/ULC listed system.*

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] - [029].

Table 11: 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.

Receiver Diagnostic Testing

[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.

Table 12: 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		
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 14 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

Table 13: 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 you need to see the IP address was assigned to the device by the DHCP Server. 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 you need to see the IP address that was assigned to the device by the DHCP server. 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 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).

[007] DNS Server IP 1

Programming not permitted on UL/ULC listed system.

Default (000.000.000.000)

|___|___|___|___|___|___|___|___|___|___|___|___|

[008] DNS Server IP 2

Programming not permitted on UL/ULC listed system.

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] System Firmware Update Fail

Default (FF) Program 00 disable or FF enable.

|___|___|

[034] Communicator Firmware Update Successful

Default (FF) Program 00 disable or FF enable.

|___|___|

[035] Panel Firmware Update Begin

Default (FF) Program 00 disable or FF enable.

|__|__|

[036] Panel Firmware Update Successful

Default (FF) Program 00 disable or FF enable.

|__|__|

[037] System 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 Access Code

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.

Programming not permitted on UL/ULC listed system.

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 ( )

Programming not permitted on UL/ULC listed system.

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.

|__|__|__|__|__|__|

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

|___|___|

LIMITED WARRANTY

Digital Security Controls (DSC) warrants the original purchaser that for a period of twelve (12) 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; or
- 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: freight cost to the repair centre; products which are not identified with DSC's product label and lot number or serial number; or 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. 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.

End User Licence Agreement

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 (DSC),** a division of Tyco Safety Products Canada Ltd., 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 EULA 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, under the following terms:.

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.

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.

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 reexport 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.

7. 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 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, 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 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 modify 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 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.

FCC Compliance Statement

CAUTION: Changes or modifications not expressly approved by the 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.

Warning: To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 20cm or more must be maintained between the antenna of this device and persons during device operation.

Industry Canada Statement

The prefix 'IC:' in front of the radio certification number signifies only that Industry Canada technical specifications were met.

Certification Number IC: 160A-3G260R

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following tow conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est conforme avec Industrie Canada exempts de licence standard RSS (s). Le fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne peut pas provoquer d'interférences et (2) cet appareil doit accepter toute interférence, y compris les interferences qui peuvent causer un mauvais fonctionnement de l'appareil.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

29008864R001