TL255

INTERNET ALARM COMMUNICATOR

Internet Communicator - North America

Installation Manual
v3.0

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, barbeques, 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 INFORMATION

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 DATA FROM KEYPAD

To enter data at the keypad, press the number key, from the table below, to select the character that you want. Pressing the number key repeatedly will scroll through the characters available for that key. Press the [*] key and use [<] [>] keys to scroll to one of the following selections: (Press [*] to select the Option.)

- **ASCII Entry.** Use this mode to enter ASCII characters from the keypad.
- **Clear to End.** This selection will clear the remainder of the display.
- **Clear Display.**This selection will completely erase all entries on the display.
- **Change Case**. Toggles between upper/lower case depending on current selection.

NOTE: The "**0**" on the keypad is used to **delete** characters.

Table 1: Data Entry at Keypad

Key	Value	Key	Value	Key	Value
1	1-A-B-C	4	4-J-K-L	7	7-S-T-U
2	2-D-E-F	5	5-M-N-O	8	8-V-W-X
3	3-G-H-I	6	6-P-Q-R	9	9-Y-Z-0

ENTERING ASCII CHARACTERS

To enter American Standard Code for Information Interchange (ASCII) characters at the keypad, perform the following:

1. Press [*] and use [<] [>] keys to scroll to "ASCII Entry".
2. Press [*] to select ASCII entry mode.
3. Use the [<] [>] keys to scroll to display the ASCII character you want to use and press [*] to accept.
4. Press [*] to exit ASCII character entry mode and return to normal entry.

MOUNTING CONSIDERATIONS

The 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 it must be 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!

The Installer must instruct the System user on each of the following items:

- This manual shall be used in conjunction with the Alarm controller manual; All the safety instructions specified within that manual shall be observed.
- 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 trained service person only.
- Use authorized accessories only with this equipment.

COMMUNICATOR TECHNICAL SPECIFICATIONS

GENERAL INFORMATION

All versions of the Internet Alarm Communicator are housed inside the Self Contained Wireless (SCW) 9055/9057.
Each version of Alarm Communicators covered by this Installation Manual are described below:
TL255: Is an Internet Alarm Communicator that sends alarm communication to Sur-Gard System I, II, III, and IV central station receivers through an Ethernet connection.
The Communicator can be used as either a backup or primary Communicator. The Communicator supports Internet Protocol (IP) transmission of panel and internal events over an Ethernet connection.

NOTE: For North America the following model name is available: **TL255**.

CAUTION:

- Do not touch any exposed wires and other conductive surfaces.
- Recycle the battery according to the local rules and regulations.

FEATURES

- 128-bit Advanced Encryption Standard (AES) encryption via Internet.
- LAN/WAN 10/100 BaseT.
- Full event reporting to central station.
- Periodic test transmission.
- Integrated call routing.
- Remote Firmware upgrade capability of the Communicator and Panel Firmware via Internet.
- CID and SIA format reporting.
- Supervision heartbeats via Internet.

UL/ULC INSTALLATION REQUIREMENTS

- For ULC Residential fire and burglary applications the **TL255** can be used as primary communication channel via Internet or as a back-up in conjunction with the Digital Alarm Communicator Transmitter (DACT). Test transmission every 24hours shall be enabled on each channel.
- For UL Residential fire and burglary applications the **TL255** can be used as primary communication channel via Internet, or as a back-up in conjunction with the DACT. (30 day test transmission is required on each channel).

RATINGS

Table 2: Communicator Electrical Ratings

Model	TL255
Power Supply Ratings	
Input Voltage	3.5 / 3.9 / 4.2 VDC (min / NOM / MAX) from the SCW panel
Current Consumption	100 mA
Standby Current (@ 3.7V)	100 mA
Alarm (Transmitting) Current)	120 mA
Environmental Specifications	
Operating Temperature	*0°C - 49°C (32°F- 120°F)*
Humidity	5% ~ 85% relative humidity, non-condensing
Mechanical Specifications	
Board Dimensions (mm/inches)	100mm x 110mm / 4.00in. x 4.25in.
Weight (grams/ounces)	55g / 1.94oz.

HARDWARE COMPATIBILITY

Table 3: Compatibility

Communicator	Receiver/ ControlPanel	Description
TL255	Receiver	SG System I, v1.14+ SG System II, v2.11+ SG-DRL3-IP, v2.3+ SG-DRL4-IP, v1.2+
	Control Panel	SCW9055/SCW9057 V1.00+

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 internal 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.

SOFTWARE COMPATIBILITY

The Communicator is compatible with the following software:

- DLS 5.

COMMUNICATOR PRE INSTALLATION CONFIGURATION

Before leaving the installation site, the Communicator TL255 shall be connected via an APPROVED (acceptable to the local authorities) Network Interface Device (NID) (e.g., for UL Installations, U60950 listed NID). All wiring shall be performed according to the local electrical codes.

ENCRYPTION

The Communicator uses 128 Bit AES Encryption. Encryption can only be enabled from the monitoring station receiver. Each receiver 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 CONFIGURATION WITH SCW

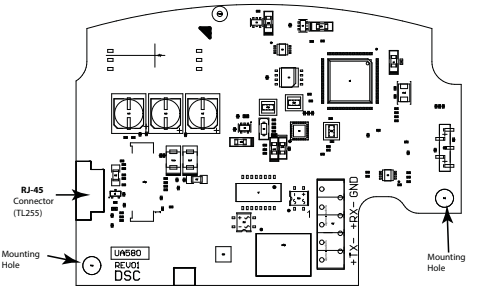
INSTALLATION LOCATION

The Communicator shall be installed in an indoor location only.

This Communicator shall be installed by Service Persons only. (Service Person is defined as a person having appropriate technical training and experience necessary to be aware of hazards to which that person may be exposed in performing a task and of 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, over voltages category II, in non-hazardous, indoor locations only. This manual shall be used with the Installation Manual of the alarm control panel which is connected to the Communicator. All instructions specified within the control panel manual must be observed.

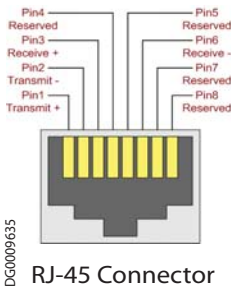
All the local rules imposed by local electrical codes shall be observed and respected during installation.

Figure 1: Communication Board Connection Points



INSTALLING CAT 5 CABLE (TL255)

Figure 2: RJ-45 Pinout



A Category 5 (CAT 5) ethernet cable must be run from a source with Ethernet/Internet connectivity to the Communicator module, inside the Self Contained Wireless Control Panel cabinet. The Communicator end of the cable must have an RJ-45 plug, which connects to the Communicator's RJ-45 jack. 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 1.2cm (½").
- 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 5 cm (2 in.) bend radius. Maximum length of CAT 5 cable is 100m (328 ft.).

NOTE: The Ethernet cable shall not be visible when the installation is complete unless the install is a surface mount installation.

COMMUNICATOR RESET

The Communicator can be reset by cycling the power on the SCW.

ESTABLISHING A COMMUNICATION CHANNEL WITH THE SCW PANEL.

The Communicator interfaces to the SCW through a keyed 16 pin Ribbon cable. See Table 4 . The key prevents incorrect connection of the ribbon cable connector to the SCW and Communicator. The pinout for the Ribbon cable is provided in the Table below:

Table 4: Communicator Ribbon cable to SCW

Pin #	Signal	Pin #	Signal
1	PC-Link TX	2	PC-Link RX
3	GND	4	Vref
5	Vref	6	GND
7	Not Used	8	Not Used
9	Not Used	10	Not Used
11	GND	12	SI
13	GND	14	SO
15	GND	16	Wall Tamper

Establishing a communication channel between the Communicator and the SCW is critical to ensuring the desired operation of the two units. The following steps must be completed during the on-site installation. Program the following to ensure that the Communicator and the panel will work together as intended.

Initial Programming of Communicator and SCW

1. Enter **[*][8][Installer Code] [Section Number]** for panel programming. Record any values that are modified from their default, in the appropriate Programming Worksheets.

NOTE: When programming Toggle Options, the toggle is ON when the number is displayed and OFF when the number is not dis played. (e.g., [1 - - - 5 - - -], Toggle Options 1 and 5 are ON, all others are OFF).

2. Panel Section **[167]** Cellular/Ethernet Interface Communications 'Wait for ACK': Default value is: **060** seconds.
3. When the communicator is installed with the SCW panel, 4 telephone numbers are available to backup one another. You can set up these 4 telephone numbers to perform in one of two ways: Backup dialling or Alternate dialling.
   a. **Backup dialling**: each of the 4 telephone numbers will make 5 dialling attempts in turn, before an FTC trouble is displayed on the keypad.
   b. **Alternate dialling**: each telephone number makes 1 dialling attempt before moving on to the next number, cycling through each of the 4 numbers for a total of 5 times each. If all 4 numbers fail the 5 attempts, an FTC trouble is displayed on the keypad.
4. Panel Sections **[301], [302], [303], and [305]** can be configured as Primary communication paths.
   a. Panel Sections **[302], [303],** and **[305]** may also be configured for backup or redundant communications by using Panel Section(s) **[383]** or **[351] - [376]**. Refer to the SCW panel Installation Manual for more information.
   b. If a valid telephone number is programmed, communications will use Public Switched Telephone Network (PSTN). Entering a 4 digit hexadecimal value for a telephone number will change the call routing to the Communicator, as determined by the number programmed:
      DCAAF: Internal (All Receivers). Signals will be routed depending on Section [851] [006] programming.
      DCBBF: Ethernet Receiver 1 (Primary).
      DCCCF: Ethernet Receiver 2 (Backup).

NOTE: Add a single 'F' as a suffix to the 4 digit hex number to populate the unused remainder of the 32 character field.

5. Panel Section **[350]**: If any of the phone numbers have been programmed as DCAA, DCBB, or DCCC, panel Section [350] must be set to [04] if SIA format or [03] if Contact ID (CID) format is used by control panel.
6. Panel Section **[382]**: Toggle Option **[5]**, 'Alternate Communicator Module Enabled', must be set to **ON**.
7. Panel Section **[401]**: Toggle Option **[1]** must be set to **ON** in order to perform panel DLS session through Ethernet data channel.
8. Panel section **[310]**, account code, auto syncs with the communicator account code in section **[021]**. The panel account code ([*****][**8**][installer code] **[310]**), will overwrite the communicator account code section ([*****][**8**][installer code] **[850] [021]**) if programmed differently.

PROGRAMMING OPTIONS

The Programming Sections described in this document can be viewed at the SCW LCD. To start programming enter: **[*][8][installer code] [851][###]**, where ### 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 your 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 or Cellular 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] and [225].

[005] System Toggle Options

[1] Ethernet Receiver 1 Supervised

Default (OFF)

(**TL255**).

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 re-sent 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 cannot be supervised.

[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.

[6] Remote Firmware Upgrade

Default (ON)

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

OFF: The Communicator module firmware cannot 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.

[006] System Toggle Options 2

[1] Ethernet 1 Receiver Enabled.

Default (ON) (OFF for **3G2055**).

ON: Ethernet Receiver 1 is enabled.

OFF: Ethernet Receiver 1 is disabled.

[2] Ethernet 2 Receiver Enabled.

Default (ON) (OFF for **3G2055**).

ON: Ethernet Receiver 2 is enabled.

OFF: Ethernet Receiver 2 is disabled.

[3] Reserved. ( ).

[6] Reserved ( ).

[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

[011] Installer Code

Default (CAFE)

Program your installer code for this 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.

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.

[020] Time Zone

Default (00)

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 5: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location	HEX Value	Offset Hours	Std Abbrev	Location
01	-12	BIT	Baker Island Time	47	5.5	IST	Indian Standard Time
05	-11	NUT	Niue Time	48	5.75	NPT	Nepal Time
		SST	Somoa Standard Time	49	6	XJT	Xinjiang Standard Time
09	-10	HAST	Hawaii-Aleutian Standard Time			EKST	East Kazakhstan Standard Time
		THAT	Tahiti Time			LKT	Sri Lanka Time
		TKT	Tokelau Time			VOST	Vostok Time
		CKT	Cook Island Time			OMSK	Omsk Standard Time
0B	-9.5	MIT	Marquesas Island Time			NOVT	Novosibirsk Time
0D	-9	AKST	Alaska Standard Time			BTT	Bhutan Time
		GIT	Gambier Island Time			BIOT	British Indian Ocean Time
11	-8	PST	Pacific Standard Time	4B	6.5	CCT	Cococ Islands Time
		PST	Pitcairn Standard Time			MMT	Myanmar Time
		CIST	Clipperton Island Standard Time	4D	7	CXT	Christmas Island Time
15	-7	MST	Mountain Standard Time			KOVT	Khovd Time
19	-6	CST	Central Standard Time			KRAT	Krasnoyarsk Time
		GALT	Galapagos Time			WIB	Waktu Indonesia Bagian Barat
		PIT	Peter Island Time			ICT	Indochina Time
		EAST	Easter Island Standard Time			BDT	Bangladesh Standard Time

Table 5: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location	HEX Value	Offset Hours	Std Abbrev	Location
1D	-5	EST	Eastern Standard Time	51	8	AWST	Australian Western Standard Time
		COT	Colombia Time			CST	China Standard Time
		ECT	Ecuador Time			HKST	Hong Kong Standard Time
		PET	Peru Time			WITA	Waktu Indonesia Bagian Tengah
		ACT	Acre Time			TWT	Taiwan Time
1F	-4.5	VST	Venezuela Standard Time			SST	Scarborough Shoal Time
21	-4	AST	Atlantic Standard Time			SIT	Spratly Island Time
		CLST	Chile Standard Time			SGT	Singapore Time
		BWST	Brazil Western Standard Time			PST	Philippine Standard Time
		SLT	San Luis Time			PIT	Pratas Islands
		PYT	Paraguay Time			PIT	Parcel Island Time
		JFST	Juan Fernandez Island Standard Time			MYT	Malaysia Time
		GYT	Guyana Time			MNT	Mongolia Time
		FKST	Falkland Island Standard Time			MBT	Macclesfield Bank Time
		BOT	Bolivia Time			IRKT	Irkutsk Time
23	-3.5	NST	Newfoundland Standard Time			BDT	Brunei Time
25	-3	CGT	Central Greenland Time			ACIT	Ashmore and Cartier Island Time
		ART	Argentina Time	52	8.25	APO	Apo Island Time
		BRT	Brazilia Time	54	8.75	ACWST	Australian Central Western Standard Time
		UYT	Uruguay Standard Time	55	9	YAKT	Yakutsk Time
		SRT	Suriname Time			JST	Japan Standard Time
		ROTT	Rothera Time			KST	Korea Standard Time
		PMST	St. Pierre & Miquelon Standard Time			WIT	Waktu Indonesia Bagian Timur
		GFT	French Guiana Time			TPT	East Timor Time
29	-2	GST	South Georgia and the South Sandwich Islands			PWT	Palau Time
		BEST	Brazil Eastern Standard Time	57	9.5	ACST	Australian Central Standard Time

Table 5: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
2D	-1	EGT	Eastern Greenland Time
		CVT	Cape Verde Time
		AZOST	Azores Standard Time
31	0	WET	Western European Time
		GMT	Greenwich Mean Time **(UTC)**
		SLT	Sierra Leone Time
		IST	Ireland Standard Time
35	1	CET	Central European Time
		WAT	Western Africa Time
		BST	British Summer Time
39	2	EET	Eastern European 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
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
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	

Table 5: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location	HEX Value	Offset Hours	Std Abbrev	Location
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				

[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 shall be programmed as FF.
(e.g., Account 1234 is programmed as:1234**FF**).

NOTE: Programming this Section with all 0 or F will cause a Module Configuration Trouble.

[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. Example: **Nri0 ET001**

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

COMMUNICATIONS REPORTING CODES

Table 6: 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	001	1	3	55	001
[024] Panel Absent Trouble Restore	ER	001	3	3	55	001
[026] Ethernet 1 Test Transmission	RP	001	1	6	A3	951
[027] Ethernet 2 Test Transmission	RP	002	1	6	A3	952
[030] FTC Restore	YK	001	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 [026 - 029]

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.

Test Transmission Unique 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.

Alternate Test Transmission:
Alternate Test Transmission can be enabled or disabled in Section [005] Toggle Option [7].

[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.

[031] Priority Tamper Alarm
Program 00 to disable this event or FF to enable. This event will occur when panel tampered during the entry delay.

[032] Priority Tamper Restore
Program 00 to disable this event or FF to enable.This event will occur when panel tamper restored.

Table 7: Priority Temper Restore

Event	SIA Identifier	SIA Reporting Code	Contact ID Qualifier	Contact ID Event Code	Contact ID Reporting Code	Contact ID User/Zone
Priority Tamper	BA	000	1	1	37	000
Priority Tamper Restore	BR	000	3	1	37	000

[033] Communicator Firmware Update Begin
Default (FF);
Program 00 to disable this event transmission or FF to enable. This event will occur when the communicator firmware update begins.

[034] Communicator Firmware Update Successful
Default (FF);
Program 00 to disable this event transmission or FF to enable. This event will occur when the communicator firmware update successfully completed.

[035] Panel Firmware Update Begin
Default (FF);
Program 00 to disable this event transmission or FF to enable. This event will occur when the panel firmware update begins.

[036] Panel Firmware Update Successful
Default (FF);
Program 00 to disable this event transmission or FF to enable. This event will occur when the panel firmware is updated successfully.

[037] Panel 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 8: Panel Tamper Alarm Restore

Event	SIA Identifier	SIA Reporting Code	Contact ID Qualifier	Contact ID Event Code	Contact ID Reporting Code	Contact ID User/Zone
[033]Comm. FW Update Begin	LB	00	1	9	03	002
[034]Comm. FW Update Successful	LS	00	3	9	03	002
[035]Panel FW Update Begin	LB	00	1	9	03	003
[036]Panel FW Update Successful	LS	00	3	9	03	003
[037]Panel FW Update Fail	LU	00	1	9	04	003

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-FFFFFFFFE. Programming all **0** or all **F** will cause a Module Configuration Trouble.

NOTE: If Ethernet Receiver 1 and Cellular Receiver 1 are programmed as the same receiver (IP and port number are identical), Ethernet Receiver 1 account code will be used.

[102] Ethernet Receiver 1 DNIS

Default (000000)

The Dialled 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/Cellular 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.

Ethernet Receiver 1 and Cellular Receiver 1 may be configured to communicate to the same central station receiver. To configure the device to operate using this Common Receiver Mode functionality, program Ethernet Receiver 1 and Cellular Receiver 1, IP address and port number with identical values.

NOTE: When operating in Common Receiver Mode, Ethernet Receiver 1 account code will be used for Ethernet and Cellular.

[104] Ethernet Receiver 1 Remote Port

Default (0BF5/3061)

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

[105] Ethernet Receiver 1 Local Port

Default (0BF4/3060)

Use this Section to set the value of the 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: 0000000001- FFFFFFFFE. Programming all **0** or all **F** will cause a Module Configuration Trouble (yellow LED=12 flashes).

NOTE: If both Ethernet Receiver 2 and Cellular Receiver 2 are the same receiver (IP and port number are identical), Ethernet Receiver 2 account will be used for Ethernet and Cellular.

[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/Cellular 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.

Ethernet Receiver 2 and Cellular Receiver 2 may be configured to communicate to the same central station receiver.

To configure the device to operate using this common receiver mode functionality, program the Ethernet Receiver 2 and Cellular Receiver 2, IP address and port number with the same values. When operating in common receiver mode the Ethernet Receiver 2 account code will be used for communications over Ethernet and Cellular.

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

[114] Ethernet Receiver 2 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 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 9: 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.

[222] Cellular Login User Name

Default ( )

Some network carriers require you to provide login credentials when connecting to an APN. Program your login User Name in this Section. Format is up to 32 ASCII characters.

NOTE: This Section is not accessible via SCW keypad programming.

INTERACTIVE PROGRAMMING OPTIONS

[651] Interactive Account Code

Default (FFFFFFFFFFF)

This section is programmed as 2 fields of 6 hexadecimal numbers (12 Characters). Valid range for each field is 000000000000 ~ FFFFFFFFFFF. The Default of this section is FFFFFFFFFFFF, when it is programmed as 000000000000 or FFFFFFFFFFF, the firmware will automatically use the MAC address as the account code when communicating to iHub.

NOTE: This section should be left at default so the MAC address is used for the account code to ensure C24 Interactive functions properly.

[652] Interactive Access Code

Default (12345678)

This Section is programmed with the hexadecimal Interactive access code. Valid Range is 00000000 ~ FFFFFFFF.

[661] Interactive Baud Rate

Default (05; 115200 Baud)

This section is programmed with the baud rate used. Valid entries are provided in the table below. Default Baud rate is 115.2KB.

Hex Value	01	02	03	04	**05**
Baud Rate	9600	19200	38400	57600	**115200**

[662] Interactive Port Settings
[1] Parity Enable/Disable Toggle
Default (OFF)
ON: Parity Enabled
OFF: Parity Disabled
[2] Parity Type
Default (OFF)
ON: Even Parity Enabled
OFF: Odd Parity Enabled
[3] Stop Bits Toggle
Default (OFF)
ON: 1 Stop Bit is used
OFF: 2 Stop Bits are used
[4] Flow Control Toggle
Default (OFF)
ON: Flow Control is enabled
OFF: Flow Control is disabled

[663] Interactive Toggle Option (1 Byte)
[1] Interactive over serial Toggle
Default (ON)
ON: Interactive over serial Enabled
OFF: Interactive over serial Disabled
[5] Interactive Protocol Toggle
Default (ON)
ON: Interactive Protocol Enabled
OFF: Interactive Protocol Disabled
NOTE: Bit 1 and Bit 5 must both be ON for interactive feature to work.

RECEIVER DIAGNOSTIC TESTING

[901] Diagnostic Test Transmission

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

SYSTEM INFORMATION (READ ONLY)

NOTE: Sections [987] - [998] are provided for information (Read Only). Values in these Sections can not be modified by the Installer.

[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.

Communicator Troubleshooting

[984] Communicator Status

The communicator status sections are intended to provide the installer with real-time status of the communicator's functionality, operational readiness, failures, and potential malfunctions that may affect flawless operation of the communicator and its primary function of sending signal to the central station in case the monitored event occurs.

The communicator status is displayed in the form of a 6-digit CODE (6 hexadecimal numbers) as in the following pattern: 00000F. The range of the code is from: 00000F – 2220CF. Not all numbers in this range are assigned a status code (Some numbers are skipped, i.e. not assigned the code).

Each digit represents a status or trouble indicator (or assigned function when no trouble is present) as described below:

1. Digit 1 - Reserved
2. Digit 2 - Reserved
3. Digit 3 - Network Indicator, displays the presence (operational status) of network.
4. Digit 4 & 5 – TROUBLE INDICATOR displays the type of problem/malfunction on communicator or modules associated with and connected to communicator.
5. Digit 6 – Reserved for future use.

For example, status code 11002F – when interpreted means: there is no network trouble, and there is trouble in the communicator, Panel supervision trouble. For details see the table below:

Table 10: Communicator Status and Trouble Coding in Hexadecimal Numbers

Digit 1		Digit 2		Digit 3		Digit 4 & 5		Digit 6
				Network indicator		TROUBLE INDICATOR		Future use
0	Reserved	0	Reserved	0	Off	00	Off (No trouble)	F
1	Reserved	1	Reserved	1	On	01	Future use	F
2	Reserved	2	Reserved	2	Flashing	02	Panel supervision trouble	F
						03	Future use	F
						04	Future use	F
						05	Future use	F
						06	Ethernet Trouble	F
						07	Receiver Not Available	F
						08	Receiver Supervision trouble	F
						09	FTC Trouble	F
						0A	Future use	F
						0B	Future use	F
						0C	Module configuration Trouble	F

The communicator status codes will indicate the network status with digit 3, and the trouble status with digit 4 and 5 as indicated in table above. For example status code 00000F would display following status:

0 – Reserved code not assigned

0 – Reserved code not assigned

0 – OFF = Network indicator, network is working

00 – TROUBLE INDICATOR = there is no trouble on the communicator.

F – Future code not assigned yet. It is sixth hexadecimal digit. It could be also ' - ' (dash) instead of letter F (00000-).

In this example both signal indicators are on indicating that communicator has excellent signal level; the network indicator is OFF showing that there are no network problems and trouble indicators are both OFF indicating that there are no trouble conditions present.

Table 11: Trouble Code Indications

Trouble Indicator Digit	Possible Causes	Trouble Possible Solutions
00	No Trouble	N/A
02	Panel Supervision Trouble	Check Section [382]Toggle Option[5] is ON (Ethernet Module Enabled). Ensure the PC-LINK cable between the Panel and Communicator is connected properly (not reversed) and is securely in place.

Trouble Indicator Digit	Possible Causes	Trouble Possible Solutions
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 that the link light on the Hub/Router/ Switch is ON. If link light is OFF, try restarting 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.
07	Receiver Not Available	Ensure that the Ethernet path has internet connectivity. If you are using a static IP address make sure 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.
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.
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.
0C	Module Configuration Trouble	This indication appears when Section [021] System Account Code, Section [101], [111], [201], and [211] Receiver Account Code have not been programmed. Ensure that a valid account code has been entered in these Sections.

Communicator Troubleshooting

The table below displays the Network indicator codes and meaning of each code.

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

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 Default ( ).
|____| [3] Supervision Type Default (OFF).
|____| [4] Primary Communications Path Default (OFF) TL255.
|____| [5] Reserved Default ( ).
|____| [6] Remote Firmware Upgrade Default (ON).
|____| [7] Alternate Test Transmission Default (OFF).
|____| [8] Reserved Default ( ).

[006] System Toggle Options 2
|____| [1] Ethernet Receiver 1 Enabled Default (ON).
|____| [2] Ethernet Receiver 2 Enabled Default (ON).
|____| [3] Reserved Default ( ).
|____| [4] Reserved Default ( ).
|____| [5] Reserved Default ( ).
|____| [6] Reserved Default ( ).
|____| [7] Reserved Default ( ).
|____| [8] Reserved Default ( ).

[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 Option
Default (CAFE) Valid range: 0000 - FFFF.
|___|___|___|___|

[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.
|___|___|___|___|

[020] Time Zone
Default (CAFE) Valid range: 0000 - FFFF.
|___|___|___|___|

[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 - 029]

[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.
|___|___|

[031] Priority Tamper Alarm
Default (FF) Program 00 disable or FF enable.
|___|___|

[032] Priority Tamper Restore
Default (FF) Program 00 disable or FF enable.
|___|___|

[033] Communicator Firmware Update Begin
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] Panel Firmware Update Fail
Default (FF) Program 00 disable or FF enable.
|___|___|

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 Remote Port
Default (0BF5/3061) Valid range: 0000 - FFFF.
|___|___|___|___|

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

[115] Ethernet Receiver 2 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.
|___|___|___|___|___|___|

INTERACTIVE PROGRAMMING OPTIONS

[651] Interactive Account Code
Default (FFFFFFFFFFF) Valid: 000000000000; FFFFFFFFFFF
|___|___|___|___|___|___|___|___|___|___|___|___|

[652] Interactive Access Code
Default (12345678) Valid range: 00000000 - FFFFFFFF.
|___|___|___|___|___|___|

[661] Interactive Baud Rate
Default (05; 115200 Baud) Valid range: 01 - 05.
|___|___|

[662] Interactive Port Settings
|____| [1] Parity Enable/Disable Default (OFF).
|____| [2] Parity Type Default (OFF; Odd Parity).
|____| [3] Stop Bits Toggle Default (OFF; 2 Stop Bits).
|____| [4] Flow Control Toggle Default (OFF).
|____| [5] Reserved Default ( ).
|____| [6] Reserved Default ( ).
|____| [7] Reserved Default ( ).
|____| [8] Reserved Default ( ).

[663] Interactive Toggle Option (1 Byte)
|____| [1] Interactive Over Serial Toggle Default (ON).
|____| [2] Reserved Default ( ).
|____| [3] Reserved Default ( ).
|____| [4] Reserved Default ( ).
|____| [5] Interactive Protocol Toggle Default (ON).
|____| [6] Reserved Default ( ).
|____| [7] Reserved Default ( ).
|____| [8] Reserved Default ( ).

RECEIVER DIAGNOSTIC TESTING

[901] Diagnostic Test Transmission
|___| [1] Ethernet 1 Default (OFF).
|___| [2] Ethernet 2 Default (OFF).

SYSTEM INFORMATION (READ ONLY)

[984] Communicator Status
[988] DNS 1 IP Address
|___|___|___||___|___|___||___|___|___|___|___|___|
[989] DNS 2 IP Address
|___|___|___||___|___|___||___|___|___|___|___|___|
[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
|___|___|

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.

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.

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-3G255SM

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.

29008688R001

DSC

A Tyco International Company

Toronto, Canada · www.dsc.com
Tech Support: 1-800-387-3630 (CA, US), 905-760-3000
Printed in Canada