LE2077

LTE/3G Wireless Alarm Communicator
Installation Manual v5.1

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

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 keeps 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 operates 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 impairs 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, renders 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 are be alerted or awakened. Audible warning devices can 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.

Contents

COMMUNICATOR TECHNICAL SPECIFICATIONS

All versions of the LTE/3G Alarm Communicator, operate on a LTE/3G network and are housed inside the Self Contained Wireless Alarm System Model SCW9055/9057. The Communicators use an Internal Antenna only.

Each version of Alarm Communicators covered by this Installation Manual are described below:

LE2077: A Long-Term Evolution/Global System for Mobile (LTE/3G) wireless Alarm Communicator that sends alarm communication to Sur-Gard System I-IP, II, III (SG-DRL3-IP), IV (SG-DRL4-IP) and 5 (SG-DRL5-IP) central station receivers through an LTE/3G digital cellular network.

CAUTION:

- Do not stay close to the equipment during device operation and to do not touch any exposed wires and other conductive surfaces,
- Recycle the battery according to the local rules and regulations.

NOTE: Prior to installation of the **LE2077**, confirm with your local carrier that the LTE/3G network is available and active in the area where the Communicator is installed, and that the location provides a radio signal strength that is adequate for uninterrupted service.

FEATURES

- 128-bit Advanced Encryption Standard (AES, Certificate No. 5376) encryption through Cellular
- Activating, initializing, and remote programming through using Connect24
- Back-up or primary Cellular alarm communication
- Dual internal LTE/3G antennas
- Full event reporting to central station
- RS422 is the connection for interactive hub/gateway.
- Individual Cellular Periodic test transmission
- 2-way audio (listen-in feature) provided over Cellular
- Integrated call routing
- Remote Firmware upgrade capability of the Communicator through Cellular
- CID and SIA format reporting
- Subscriber Identity Module (SIM) card, included with Communicator
- Supervision heartbeats through LTE/3G

UL/ULC INSTALLATION REQUIREMENTS

- For ULC Residential fire and burglary applications the **LE2077** can be used as primary communication channel using Cellular (as applicable) or as a back-up in conjunction with the Digital Alarm Communicator Transmitter (DACT). Test transmission every 24 hours is required on each channel.
- For UL Residential fire and burglary applications the **LE2077** can be used as primary communication channel using Cellular or as a back-up in conjunction with the DACT. Test transmission every 30 days is required on each channel.

COMMUNICATOR FREQUENCY BANDS FOR NORTH AMERICA

Table 1: 3G Frequency Bands - North America

Transmit Direction	Cellular 850 North America	PCS 1900 North America
Transmit Frequency	824 MHz to 849 MHz	1850 MHz to 1910 MHz
Receive Frequency	869 MHz to 894 MHz	1930 MHz to 1990 MHz

Table 2: LTE Frequency Bands (model LE2077 only)

Band	Transmit Band (TX)	Receive Band (RX)
LTE B2	1850 MHz to 1910 MHz	1930 MHz to 1990 MHz
LTE B4	1710 MHz to 1755 MHz	2110 MHz to 2155 MHz
LTE B5	824 MHz to 849 MHz	869 MHz to 894 MHz
LTE B12	698 MHz to 716 MHz	728 MHz to 746 MHz
LTE B13	777 MHz to 787 MHz	746 MHz to 756 MHz
UMTS B2	1850 MHz to 1910 MHz	1930 MHz to 1900 MHz
UMTS B5	824 MHz to 840 MHz	824 MHz to 894 MHz

RATINGS

Table 3: Communicator Electrical Ratings

Model	LE2077 Cellular Only
Power Supply Ratings	
Input Voltage	3.5 / 3.9 / 4.2 VDC (min / NOM / MAX) from the SCW9055/SCW9057 panel
Current Consumption	75 mA
Standby Current (@ 3.7V)	75 mA
Alarm (Transmitting) Current)	400 mA @ 3.7V during transmission
Antenna Specifications	
Dual band Antenna	See Table 1
Environmental Specifications	
Operating Temperature	*0°C - 49°C (32°F- 120°F)*
Humidity	5% ~ 85% relative humidity, non-condensing
Mechanical Specifications	
Board Dimensions (mm)	109 x 110
Weight (grams)	60

HARDWARE COMPATIBILITY

Table 4: Compatibility

Communicator	Receiver/Control Panel	Description
LE2077	Receiver	SG System I, v1.14+ SG System II, v2.11+ SG-DRL3-IP, v2.3+ SG-DRL4-IP, v1.2+ SG-DRL5-IP, V1.0+
	Control Panel	SCW9055/SCW9057 V1.17/1.18

Note for ULC Listed installations:
Products or components of products, which perform communications functions only, must comply with the requirements applicable to communications equipment as specified in CAN/CSA –C22.2 No. 60950-1, Information Technology Equipment-Safety - Part 1: General Requirements. Where network interfaces, such as the following, are internal to the subscriber 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; Network interface devices; Third party communications service providers; Digital subscriber line (DSL) modems; and Cable modems.

Note for UL Listed installations:
Packet switched data network interface equipment, manufactured by other than the burglar alarm equipment manufacturer, that is not required for the processing of the signals must be evaluated to the applicable requirements of the Standard for Information Technology Equipment – Safety – Part 1: General Requirements, UL 60950-1, either as burglar alarm equipment or communication equipment.

COMMUNICATOR PRE INSTALLATION CONFIGURATION

CONNECT24™[1] ACCOUNT AND SIM CARD ACTIVATION

Installation of the Communicator requires activation with Connect24 before operation. The LE2077 can be initialized with C24 Communications. To complete enrollment, a C24 Communications login and the 20-digit SIM number are required.

NOTE: The SIM activation process with the cellular carrier typically takes between five and 10 minutes to complete.

ENCRYPTION

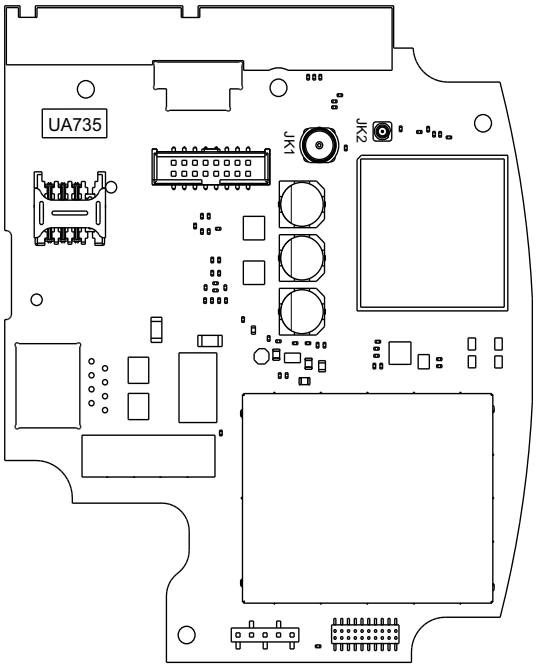
The Communicator uses 128 Bit AES Encryption. Encryption can only be enabled from the monitoring station receiver. Each receiver can independently have encryption enabled or disabled. When encryption is enabled, the central station configures the device to encrypt communications the next time the Communicator module performs a communication to that receiver.

NOTE: Packet encryption starts only after the next event is sent to that receiver, or if the unit is restarted.

1. **Connect24**, **DSC**, and **DLS IV** are Registered Trademarks of Tyco International Ltd. and its respective Companies. All Rights Reserved.

COMMUNICATOR CONFIGURATION WITH SCW9055/ SCW9057

NOTE: The SCW9055/ SCW9057 should not be mounted in its final location without performing a Communicator Test to ensure adequate LTE/ 3G coverage for the **LE2077** Alarm Communicator.



INSTALLATION LOCATION

The SCW9055/SCW9057 and integrated LE2077 alarm communicator shall be installed in an indoor location only.

This LTE/3G Communicator must be installed by Skilled Persons only. Skilled Person is defined as a person with relevant education or experience to enable him or her to identify hazards and to take appropriate actions to reduce the risks of injury to themselves and others. The Communicator must 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 must be used with the Installation Manual of the alarm control panel which is connected to the LTE/3G Communicator. All instructions specified within the control panel manual must be observed.

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

ANTENNA CONNECTIONS

JK1 – If an external antenna extension kit is required to improve cellular performance, connect the antenna extension cable to JK1. This deactivates the on-board antenna and allows the product to use the external antenna. (See Figure 1.)

JK2 – The secondary receive antenna, mounted on the right side of the product enclosure, is attached to the communicator using JK2. (See Figure 1.).

INSERTING/REMOVING THE SIM CARD

1. Remove the front cover of the SCW9055/SCW9057 Control Panel to access SIM card holder.

2. Remove power from the SCW9055/SCW9057 and disconnect the backup battery connections.
3. Gently slide the SIM card into the SIM card holder and ensure the notch in the corner of the SIM card aligns with the indication on the PCB.
4. Apply AC power to panel, and replace the panel cover.

NOTE: If two way audio is enabled you CANNOT swap the SIM card with another card.

COMMUNICATOR RESET

The Communicator can be reset by cycling the power on the SCW9055/SCW9057.

ESTABLISHING A COMMUNICATION CHANNEL WITH THE SCW9055/SCW9057 PANEL

The Communicator interfaces to the SCW9055/SCW9057 through a keyed 16-pin Ribbon cable. See Table 6 . The key prevents incorrect connection of the ribbon cable connector to the SCW9055/SCW9057 and Communicator. The pin-out for the Ribbon cable is provided in the Table below:

Table 5: Communicator Ribbon cable to SCW9055/SCW9057

Pin #	Signal	Pin #	Signal
1	PC-Link TX	2	PC-Link RX
3	GND	4	Vref
5	Vref	6	GND
7	AUD-OUT_N	8	AUD-OUT_P
9	AUD-IN_P	10	AUD-IN_N
11	GND	12	SI
13	GND	14	SO
15	GND	16	Wall Tamper

Establishing a communication channel between the Communicator and the SCW9055/SCW9057 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 options to ensure that the Communicator and the panel work together as intended.

Initial Programming of Communicator and SCW9055/SCW9057

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 displayed. (e.g., [1 - - - 5 - - -], Toggle Options 1 and 5 are ON, all others are OFF).

2. Panel section **[167]** Cellular Interface Communications 'Wait for ACK': Default value is: **060** seconds.
3. When the communicator is installed with the SCW9055/SCW9057 panel, four telephone numbers are available to backup one another. You can set up these four telephone numbers to perform in one of two ways: Backup dialing or Alternate dialing.
   a. **Backup dialing**: Each of the four telephone numbers make five dialing attempts in turn, before an FTC trouble is displayed on the keypad.
   b. **Alternate dialing**: each telephone number makes one dialing attempt before moving on to the next number, cycling through each of the four numbers for a total of five times each. If all four numbers fail the five 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 SCW9055/SCW9057 panel Installation Manual for more information.

b. If a valid telephone number is programmed, communication uses Public Switched Telephone Network (PSTN). Entering a 4-digit hexadecimal value for a telephone number changes the call routing to the Communicator, as determined by the number programmed:

DCAAF: Internal (all receivers). Signals are routed depending on section [851] [006] programming.

DCDDF: Cellular Receiver 1 (Primary).

DCEEF: Cellular 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, DCDD, or DCEE, 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]**, 'GS/IP 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 Cellular 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]**) overwrites the communicator account code section ([*][**8**][installer code] **[851] [021]**), if programmed differently.

NOTE: Keep a record of the SIM card telephone number as it is required by users for SMS Command and Control functions. (The number can be recorded in the Programming Worksheets Section of this document, under Option **[996]**.) Due to the nature of the SIM card activation process with Cellular network carriers, it can take up to 24 hours for SIM card activation to be complete.

COMMUNICATOR PLACEMENT TEST

1. Using the keypad enter the installer mode: [*][8] [installer code] [850].
2. View and record the number of bars showing on the SCW9055/SCW9057 LCD.
3. Compare with the number of bars indicated in the CSQ Levels column in Table 6.
4. If three or more bars are shown, the location is GOOD for installation.
5. If the location is BAD, move the SCW9055/SCW9057 to various suitable locations until three or more bars are obtained.

Table 6: ***Communicator CSQ Levels***

Signal Strength	CSQ Level	Signal Level dBm	Installer Action
5 Bars	14 and higher	-84 and higher	Location is GOOD.
4 Bars	11 to 13	-90 to -85	
3 Bars	7 to 10	-98 to -91	
2 Bars	5 to 6	-102 to -99	Location is BAD. Not suitable for Cellular operation.
1 Bar	1 to 4	-108 to -103	
No Signal	0	-108.8	Check if Cellular coverage is active in your area.

CELLULAR PROGRAMMING OPTIONS

The Programming Sections described in this document can be viewed at the SCW9055/ SCW9057 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.

Programming sections are accessed through using Connect24. Installers can **review/record** programming Options at the panel.

NOTE: Cellular Programming Sections accessed through the panel are for **display purposes only**. Configuration changes must be done using Connect24.

SYSTEM OPTIONS

[004] Receiver Supervision Interval

Default (0087/135)

When receiver supervision is enabled (ON) in section [005], toggle option [3], the unit sends heartbeats to Cellular Receiver 1 to test the communications path. Use this section to set the interval time (in seconds) when heartbeats are 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]. When programming using Connect24, the recommended intervals are programmed automatically when the required window is selected.

[005] System Toggle Options

[2] Cellular Receiver 1 Supervised

Default (OFF)

ON: Cellular Receiver 1 is supervised and heartbeats are sent to Cellular Receiver 1 based on the supervision interval programmed in section [004]. If ACK to heartbeat is not received, it is retransmitted every 5 seconds. Failure to ACK 2 consecutive heartbeats resets the radio.

OFF: Cellular Receiver 1 is not supervised. When disabled, heartbeat is not sent to the receiver. Supervisory trouble is indicated.

NOTE: Cellular 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 must 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 Cellular 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.

[8] Cellular Low Signal Trouble.

Default (OFF)

This option masks the Low Signal trouble from the Cellular trouble event.

ON: A Cellular Trouble event is transmitted to receiver when the radio signal level falls below threshold level (average CSQ level is 4 or less).

OFF: A Cellular Trouble event is **not** transmitted to receiver when the radio signal level falls below threshold level (average CSQ level is 4 or less).

[006] System Toggle Options 2

[3] Reserved. ( ).

[4] Cellular 1 Receiver Enabled.

Default (ON).

ON: Cellular Receiver 1 is enabled.

OFF: Cellular Receiver 1 is disabled.

[5] Cellular 2 Receiver Enabled.

Default (ON).

ON: Cellular Receiver 2 is enabled.

OFF: Cellular Receiver 2 is disabled.

[6] Reserved ( ).

[7] DLS Over Cellular.

Default (**ON**).

NOTE: Program this toggle as OFF if you want to completely disable DLS from using the Cellular path.

ON: DLS is enabled on the Cellular path.

OFF: DLS is disabled on the Cellular path.

NOTE: If this Toggle is OFF, DLS sessions occur on the Cellular path, regardless of Primary Path set in section [005], toggle option [4]. If it is ON, the Communicator connects to the Primary path first for DLS. If the session fails, the Secondary path is used.

[8] Reserved ( ).

PROGRAMMING OPTIONS

[010] System Toggle Option

Default (Disable)

[1] This bit is used to enable/disable two way audio over Cellular.

[011] Installer Code

Default (CAFE)

Program your installer code for this Communicator module. The installer code is 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 5 uses 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 5 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.

[020] Time Zone

Default (00)

Use Column 2 (Offset Hours) to find your local Time Zone. Record the 2-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 7: 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	Pitcairn 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
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

Table 7: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
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 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

Table 7: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
45	5	CAST	Chinese Atlantic Standard Time
		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
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
		IRKT	Irkutsk Time
		BDT	Brunei Time
		ACIT	Ashmore and Cartier Island Time
52	8.25	APO	Apo Island Time
54	8.75	ACWST	Australian Central Western Standard Time

Table 7: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location
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
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: 00000**1**-FFFFF**E**. If 4-digit account codes are needed the two lowest digits must be programmed as FF.
(e.g., Account 1234 is programmed as:1234**FF**).

NOTE: Programming this section with all 0 or F causes 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 sends the account code along with its data transmission. The transmission looks 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 8: 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
[025] Radio Activation Restore	RS	001	3	5	52	001
[028] Cellular 1 Test Transmission	RP	003	1	6	A3	955
[029] Cellular 2 Test Transmission	RP	004	1	6	A3	956
[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 occurs 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 occurs when communications with the control panel have resumed.

[025] Radio Activation Restore

Default (FF)

Program 00 to disable this event or FF to enable. This event occurs after any successful programming session (using Connect24).

SYSTEM TEST OPTIONS [026 - 029]

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

Set Cellular Section [028] to (FF); [029] to (00).

- If the test transmission fails to the primary receiver, it backs up to the secondary receiver.
- If the test transmission fails to the secondary receiver, an FTC trouble is generated.

Test Transmission Unique to Primary and Secondary Receivers:

Set Cellular Section [028] to (FF); [029] to (FF).

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

Alternate Test Transmission:

Alternate Test Transmission can be enabled or disabled in section [005], toggle option [7].

[028] Cellular 1 Transmission

Default (FF)

Program 00 to disable this event transmission or FF to enable. See System Test Options (above) for details on settings.

[029] Cellular 2 Transmission

Default (00)

Program 00 to disable this event transmission or FF to enable. See System Test Options (above) for details on settings.

NOTE: The time interval (in minutes) between periodic tests is programmed in section [225] (Cellular).

[030] FTC Restore

Default (FF)

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

[031] Priority Tamper Alarm

Program 00 to disable this event or FF to enable. This event occurs when panel tampered during the entry delay.

[032] Priority Tamper Restore

Program 00 to disable this event or FF to enable. This event occurs when panel tamper restored.

Table 9: 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 occurs 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 occurs when the communicator firmware updated successfully completed.

[035] Panel Firmware Update Begin

Default (FF);

Program 00 to disable this event transmission or FF to enable. This event occurs 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 occurs when the panel firmware updated successfully.

[037] Panel Firmware Update Fail

Default (FF);

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

Table 10: 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

CELLULAR RECEIVER 1 OPTIONS

[201] Cellular 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 control panel use the control panel account number. Valid range: 0000000001 - FFFFFFFFFE. Programming all **0** or all **F** causes a Module Configuration Trouble (yellow LED = 12 flashes).

[202] Cellular Receiver 1 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. Values are entered as leading **0** followed by the 5-digit DNIS. Format is BCD.

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

[203] Cellular Receiver 1 Address

Default (000.000.000.000)

Enter the Cellular Receiver 1 IP address. This information is provided by your central station system administrator. Each 3-digit segment of the address must be within a valid range of 000-255.

NOTE: When a valid IP address has been entered, the Cellular is enabled and communicates events over the Cellular channel.

[204] Cellular Receiver 1 Port

Default (0BF5/3061)

This section determines the port used by Cellular Receiver 1. Change the default 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: Programming this section with 0000 disables the receiver.

[205] Cellular Receiver 1 APN

Default ( )

The Access Point Name (APN) determines the Cellular network that the Communicator connects to. This information is available from your network carrier. Program this Section as 32 ASCII characters.

NOTE: When a SIM card with a custom APN is used, the unit cannot access the Internet. DLS and remote flash can still be done if section [221] is programmed with a valid Public APN.

[206] Cellular Receiver 1 Domain Name

Default ( )

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

Enter the Domain Name as 32 ASCII characters. This information is provided by your central station system administrator.

CELLULAR RECEIVER 2 OPTIONS

[211] Cellular Receiver 2 Account Code

Default (0000000000)

The account code is used by the central station to distinguish between different transmitters. This account code is used when transmitting signals to the central station receiver. Signals received on the panel use the panel account number. Valid range: 000000000**1** - FFFFFFFF**E**.

NOTE: Programming this section as all 0 or F causes a Module Configuration Trouble (yellow LED = 12 flashes).

[212] Cellular 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 - **0**99999. Values are entered as a 0 followed by the 5-digit DNIS value. Format is BCD.

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

[213] Cellular Receiver 2 Address

Default (000.000.000.000)

Enter the Cellular Receiver 2 IP address. This IP address is provided by your central station. Format is four fields, each field is 3-digit decimal. Valid range: 000 - 255.

NOTE: When a valid IP address is provided, Cellular Receiver 2 is enabled and communicates events over the Cellular path.

[214] Cellular Receiver 2 Port

Default (0BF5/3061)

This section defines the port of Cellular Receiver 2. Change 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 Cellular Receiver 1 and Cellular Receiver 2 to communicate to the same receiver.

[215] Cellular Receiver 2 APN

Default ( )

The APN determines the Cellular network to which the Communicator connects. This information is available from your network carrier. Program this section with up to 32 ASCII characters.

NOTE: When a SIM card with a custom APN is used, the unit cannot access the internet. DLS and remote flash can still be done if section [221] is programmed with a valid Public APN.

[216] Cellular Receiver 2 Domain Name

Default ( )

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

Enter the Cellular Receiver 2 Domain Name with up to 32 ASCII characters.

CELLULAR OPTIONS

[221] Cellular Public Access Point Name

Default ( )

When the Communicator is operating on a private APN, use this section to select a public APN for DLS and Remote Firmware Update. This information is available from your network carrier. The APN identifies the public Cellular network to which the Communicator connects.

[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 through SCW9055/9057 keypad programming.

[223] Cellular Login Password

Default ( )

Some network carriers require you to provide login credentials when connecting to an APN. Program your login Password in this section.

Format is up to 32 ASCII characters.

[224] Cellular Test Transmission Time of Day

Default (9999)

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

NOTE: To disable the test transmission time of day enter 9999 or FFFF in this section.

The internal date and time will be automatically programmed by the primary receiver only.

[225] Cellular Test Transmission Cycle

Default (000000)

This value represents the interval in between test transmissions in minutes. Valid range: 000000 - 999999 minutes. When the unit has sent the initial periodic test transmission, all future test transmissions is offset by the programmed number of minutes. See sections [026] - [029].

Table 11: Cellular 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 disables test transmission.

[226] Cellular Trouble Delay

Default (00)

This option is used to program the delay, in minutes, for reporting a Cellular Trouble Delay. Valid entries are 00 - FF. (e.g., for a 10-minute Cellular Trouble Delay enter: **0A**). There is no reporting delay if value is programmed as 00.

[227] Voice Call Timeout

Default (00)

This option sets the Voice Call Timeout in minutes. Programming a value of 00 disables timeout. Valid range is 00 to FF.

[228] Voice Call Back Time

Default (0A)

This option sets the voice call back time in minutes. When the Communicator requests Call Back from the receiver, it answers incoming calls during the programmed timeout period. If an incoming call is received after the timeout from requesting call back, the Communicator answers the call and immediately hang up. Programming a value of 00 disables timeout (accept all incoming calls). Default value is 0A/10 seconds. Valid range is 00 to FF.

[229] Voice Call Back Number

Default (SIM Telephone Number)

This option sets the Voice Call Back Telephone Number for the receiver. This number is used for Two Way calling. Current SIM telephone number can be viewed in section [996]. Valid entry is 32 character ASCII.

RECEIVER DIAGNOSTIC TESTING

[901] Diagnostic Test Transmission

[3]	Cellular 1	(OFF).
[4]	Cellular 2	(OFF).
[5],[6],[7],[8]	Reserved	(OFF).

Use this section 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 indicates 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 cannot be modified by the Installer.

[987] Language Version

This section displays the current Language version of the Communicator.

[988] DNS 1 IP Address

This section displays 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 assigned by DHCP.

[989] DNS 2 IP Address

This section displays 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 assigned by DHCP.

[990] Boot Loader Version

This section displays the current Boot Loader version of the Communicator.

[991] Firmware Version

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

[994] Cellular IP Address

This section displays the current dynamic IP address assigned by DHCP to the Cellular connection.

NOTE: Cellular uses DHCP (Dynamic IP) only. The Cellular IP address is always provided by the Cellular network (i.e., not programmable).

[995] SIM Number

This section displays the Subscriber Identity Module (SIM) number of the SIM card installed in the Communicator. Format is: Major Industry Identifier (2 digits) Mobile Country Code (2 or 3 digits); Mobile Network Code (2 - 3 digits); Unique Number (10 - 12 digits); and Checksum (1 digit). Valid SIM numbers range is: 18 - 21 numbers. This number is printed on SIM and the outside of the Communicator carton.

NOTE: The Checksum digit is omitted on 19-digit SIM Card numbers.

[996] Cellular Telephone Number

NOTE: This section displays the Cellular telephone number of the SIM. This telephone number is required by the Installer for DLS and remote firmware (flash) update. User can access this telephone number by entering [*] [6] < > SMS Programming [*] and select Phone No. 1 to display the phone number.

[997] IMEI Number

This section displays the unique 15-digit International Mobile Equipment Identity (IMEI) of the radio. Format is: Reporting Body Identifier (2 digits), Allocation Number (4 digits); Final Assembly Code (2 digits); Serial Number (6 digits); and a check digit.

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 erases all existing programming of the unit.

55: **Reset**. The Communicator is reset. This option is equivalent to power cycling the Communicator.

Communicator Troubleshooting

[980] Cellular Technology

The cellular technology section is intended to allow the installer to easily check what network technology and signal strength the communicator currently has, as well as display the technology used in the last two-way voice call the communicator has made.

The top line of this section displays which network technology (LTE or 3G) is currently in use and which was used for the last voice call. It also shows a CSQ value for signal strength (0-31).

NET:LTE CSQ 30

Last 2WV:LTE

[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 can 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 - Signal Indicator 1, displays the presence/strength of signal 1.
2. Digit 2 - Signal Indicator 2, displays the presence/strength of signal 2.
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: "Signal Indicator 1 OK, Signal indicator 2 OK, there is no network trouble, and there is trouble in the communicator, Panel supervision trouble." For details see the table below:

Table 12: Communicator Status and Trouble Coding in Hexadecimal Numbers

Digit 1		Digit 2		Digit 3		Digit 4 & 5		Digit 6
Signal indicator 1		Signal indicator 2		Network indicator		TROUBLE INDICATOR		Future use
0	Off	0	Off	0	Off	00	Off (No trouble)	F
1	On	1	On	1	On	01	Future use	F
2	Flashing	2	Flashing	2	Flashing	02	Panel supervision trouble	F
						03	Future use	F
						04	Lockout trouble	F
						05	3G/Cellular trouble	F

Digit 1		Digit 2		Digit 3		Digit 4 & 5		Digit 6
						06	Future use	F
						07	Receiver Not Available	F
						08	Receiver Supervision trouble	F
						09	FTC Trouble	F
						0A	C24 Configuration SMS Failure	F
						0B	Future use	F
						0C	Module configuration Trouble	F

The communicator status codes indicate the signal levels with digit 1 and 2, a network status with digit 3, and the trouble status with digit 4 and 5 as indicated in table above. For example status code 11000F displays following status:

1 – On = Signal indicator 1, is ON

1 – On = Signal indicator 2, is ON

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 (11000-).

In this example both signal indicators are on indicating that communicator has excellent signal level; the network indicator is OFF showing that we do not have any network problems and trouble indicators are both OFF indicating that we don’t have any trouble on the communicator.

[985] Radio Initialization Status

The radio initialization status is intended to provide the installer with real time status of radio communication. The radio initialization status is displayed in 8-bit toggle option. Each digit indicates one task in radio initialization process that is complete step in entire process of radio initialization as following:

1. Radio power up
2. Received the SMS from C24
3. Radio reset
4. Radio attached to network
5. Not used
6. Not used
7. Receiver 3 Initialized
8. Receiver 4 Initialize

The following table shows each digits position in status code and each digit value and its assigned meaning in the 8-digit code:

Table 13: Radio Initialization Status - 1-8 bits completion

Bit	1	2	3	4	5	6	7	8
Not Completed	-	-	-	-	-	-	-	-
Completed	1	2	3	4	5	6	7	8

For example, the radio initialization status code 12-45--- indicates that Radio has been powered up, it has received SMS signal from C24, the radio is attached to the network, and Receiver 1 has been initialized. This code could be followed with...567 if Receivers 2, 3, and 4 are initialized where applicable.

If the radio initialization status code does not indicate any problems, proceed with installation as per this manual. If troubles are reported, reset the initialization process. If this action does not fix the problem, refer to Troubleshooting section in this manual.

Table 14: 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. (LTE/3G/ Module Enabled) Ensure the ribbon cable between the Panel and Communicator is connected properly (not reversed) and is securely in place.
05	LTE/3G Cellular Trouble	Confirm that LTE/3G service is available and active in your area. Check all antenna connections. Ensure average radio signal strength is CSQ 7 or higher. (See Table 7). Ensure the SIM card is properly inserted into the SIM card holder. Ensure the SIM card has been activated. (Could take up to 24 hrs after install). If this trouble persists, relocate the Panel (and Communicator) or install an external antenna extension kit.
07	Receiver Not Available	Ensure that the communication 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. Ensure the LTE/3G Receiver APNs have been programmed with the Access Point Name provided by your LTE/3G provider.
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 receiver for events generated by the Communicator. Restart the system, if trouble persists, contact your dealer.
0A	Connect24 Configuration Failure	The SIM is active but there is no programming for the Communicator. Ensure a profile has been programmed in Connect24 for the SIM. You can confirm your programming by calling the Connect24 VRU, or by logging into the Connect24 VRU web site.
0C	Module Configuration Trouble	This indication appears when section [021] System Account Code or 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 status codes for the radio signal strength, typical troubles, possible causes, and troubleshooting instructions are displayed in the table below.

Table 15: Radio Signal Strength

Signal Strength	CSQ Level	Signal Indicator 1	Signal Indicator 2	Signal Level [dBm]	Signal Level Status	Action Required
5 Bars	14 +	1	1	-84 and higher	excellent	**Location is OK.** 3G Signal Strength is greater than CSQ 7.
4 Bars	11 - 13	2	1	-90 ~ -85	strong	
3 Bars	7 - 10	2	1	-98 ~ -91	strong	
2 Bars	5 - 6	0	1	-102 ~ -99	weak	Relocate Panel if signal strength shows less than 3 bars.
1 Bar	1 - 4	0	2	-108 ~ -103	weak	
No Signal	0	0	0	-108.8	bad	Check all antenna connections. Confirm cellular service is active in area. Relocate Panel.

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

Table 16: Network indicator - Digit 3

Network indicator Value	Means
OFF	No Network Trouble
ON	Radio connection has been restored. Radio IP failed
Flashing	Incoming transmission Connect 24 programming Outgoing transmission Incoming transmission

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 alternately turns 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,

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 scrolls 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 clears the remainder of the display.
- **Clear Display.**This selection completely erases 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 16: 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 the ASCII character you want to use and press [*] to accept.
4. Press [*] to exit ASCII character entry mode and return to normal entry.

NOTE: Authorized access to C24 is required to modify any Cellular Programming section. Specific panel sections must be configured for proper operation of the Communicator with the panel.

Mounting Considerations

The Cellular Communicator is fixed, wall-mounted unit and must 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 must be used in conjunction with the Alarm controller manual; All the safety instructions specified within that manual must 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 must be referred to trained skilled persons only.
- Use authorized accessories only with this equipment.

Cellular Coverage for Alarm Communicator Operation

The LTE/3G performance of the LE2077 Alarm Communicators depends greatly on Cellular network coverage. The SCW9055/SCW9057 (with internal Alarm Communicator) must not be mounted in the final location without first ensuring that Cellular radio reception is adequate for communication using the LTE/3G paths. Perform the “Communicator Placement Test” on page 9.

CELLULAR PROGRAMMING WORKSHEETS

SYSTEM OPTIONS

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

|___|___|___|___|

[005] System Toggle Options

|___| [2] Cellular Receiver 1 Supervised Default (OFF).

|___| [3] Supervision Type Default (OFF).

|___| [4] Primary Communications Path.

Default [ON]LE2077.

|___| [5] Redundant Communications Default (OFF).

|___| [6] Remote Firmware Upgrade Default (ON).

|___| [7] Alternate Test Transmission Default (OFF).

|___| [8] Cellular Low Signal Trouble Default (OFF).

[006] System Toggle Options 2

|___| [4] Cellular Receiver 1 Enabled Default (ON).

|___| [5] Cellular Receiver 2 Enabled Default (ON).

|___| [7] DLS Over Cellular Default (ON).

|___| [8] Interactive Over Cellular Default (ON).

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.

|___|___|

[025] Radio Activation Restore
Default (FF) Program 00 disable or FF enable.

|___|___|

SYSTEM TEST OPTIONS [026 - 029]

[028] Cellular 1 Transmission
Default (FF) Program 00 disable or FF enable.

|___|___|

[029] Cellular 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.

|___|___|

CELLULAR RECEIVER 1 OPTIONS

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

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

[202] Cellular Receiver 1 DNIS
Default (000000) Valid range: 000000 - 0FFFFF.

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

[203] Cellular Receiver 1 Address
Default (000.000.000.000). Valid range: 000-255.

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

[204] Cellular Receiver 1 Port
Default (0BF5/3061) Valid range: 0000 - FFFF.

|___|___|___|___|

[205] Cellular Receiver 1 APN Default ( )
32 ASCII characters.

_____

[206] Cellular Receiver 1 Domain Name
Programming not permitted on UL/ULC listed system.
Default ( ) 32 ASCII characters.

_____

CELLULAR RECEIVER 2 OPTIONS

[211] Cellular Receiver 2 Account Code
Default (0000000000)
Valid range: 000000000**1** - FFFFFFFFF**E**.

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

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

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

[213] Cellular Receiver 2 Address
Default (000.000.000.000) Valid segment range: 000-255

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

[214] Cellular Receiver 2 Port
Default (0BF5/3061) Valid range: 0000 - FFFF.

|___|___|___|___|

[215] Cellular Receiver 2 APN
Default ( ) 32 ASCII characters.

_____

[206] Cellular Receiver 1 Domain Name
Programming not permitted on UL/ULC listed system.
Default ( ) 32 ASCII characters.

_____

CELLULAR OPTIONS

[221] Cellular Public Access Point Name
Default ( ) 32 ASCII characters

_____

[222] Cellular Login User Name
Default ( ) 32 ASCII characters.

_____

[223] Cellular Login Password
Default ( ) 32 ASCII characters.

_____

[224] Cellular Test Transmission Time of day
Default (9999) Valid range: 00 - 23 hrs. (HH) 00 - 59 min. (MM).|___|___|___|___|

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

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

[226] Cellular Trouble Delay
Default (00) Program 00 disable or FF enable.

|___|___|

[901] Diagnostic Test Transmission

|___| [3] Cellular 1 Default (OFF).

|___| [4] Cellular 2 Default (OFF).

SYSTEM INFORMATION (READ ONLY)

[988] DNS 1 IP Address

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

[989] DNS 2 IP Address

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

[991] Firmware Version

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

[994] Cellular IP Address

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

[995] SIM Number

_____

[996] Cellular Telephone Number
This number is required for DLS, and Firmware upgrades.

_____

[997] IMEI Number

_____

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.

REGULATORY INFORMATION

MODIFICATION STATEMENT
Digital Security Controls has not approved any changes or modifications to this device by the user. Any changes or modifications could void the user's authority to operate the equipment.

Digital Security Controls n'approuve aucune modification apportée à l'appareil par l'utilisateur, quelle qu'en soit la nature. Tout changement ou modification peuvent annuler le droit d'utilisation de l'appareil par l'utilisateur.

INTERFERENCE STATEMENT
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two 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.

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

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radio électrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

WIRELESS NOTICE
This equipment complies with FCC and IC radiation exposure limits set forth for an uncontrolled environment. The antenna should be installed and operated with minimum distance of 20 cm between the radiator and your body.

Cet appareil est conforme aux limites d'exposition aux rayonnements de la IC pour un environnement non contrôlé. L'antenne doit être installé de façon à garder une distance minimale de 20 centimètres entre la source de rayonnements et votre corps.

Antenna gain must be below/Gain de l'antenne doit être ci-dessous:

Frequency Band/Bande de fréquence	LE2077
GSM850 / FDD V	2.10 dBi
PCS1900 / FDD II	1.90 dBi
LTEB2	1.90 dBi
LTEB4	1.60 dBi
LTEB5/B12/B13	2.1/ - 1.8/0 dBi

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
L'émetteur ne doit pas être colocalisé ni fonctionner conjointement avec à autre antenne ou autre émetteur.

FCC CLASS B DIGITAL DEVICE NOTICE
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:

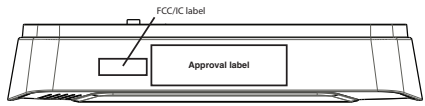
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAN ICES-3 (B)/ NMB-3 (B)
FCC ID: F5318LE2077
IC:160A-LE2077

FCC/IC LABEL
This modular transmitter is labeled with its own FCC ID and IC number. When the module is installed inside the host device and the FCC ID/IC of the module is not visible, the host device shall display the provided label referring to the FCC ID and IC of the enclosed module. This label is shipped together with the module and it is the responsibility of the integrator to apply it to the exterior of the enclosure as displayed in the following figure.

Le modulaire émetteur 3G7090 ou LT7090 est étiqueté avec son propre ID FCC et le numéro IC. Lorsque le module est installé à l'intérieur du dispositif hôte WS900-19 ou WS900-29 et la FCC ID / IC du module ne soit pas visible, le dispositif d'accueil affiche l'étiquette fournie se référant à l'ID FCC et IC du module ci-joint. Ce label est livré avec le
module et il est de la responsabilité de l'intégrateur de l'appliquer à l'extérieur de l'enceinte, comme indiqué dans la figure suivante.

Model LE2077
Contains FCC ID: F5318LE2077
Contains IC: 160A-LE2077



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

DSC

From Tyco Security Products

29010190R001