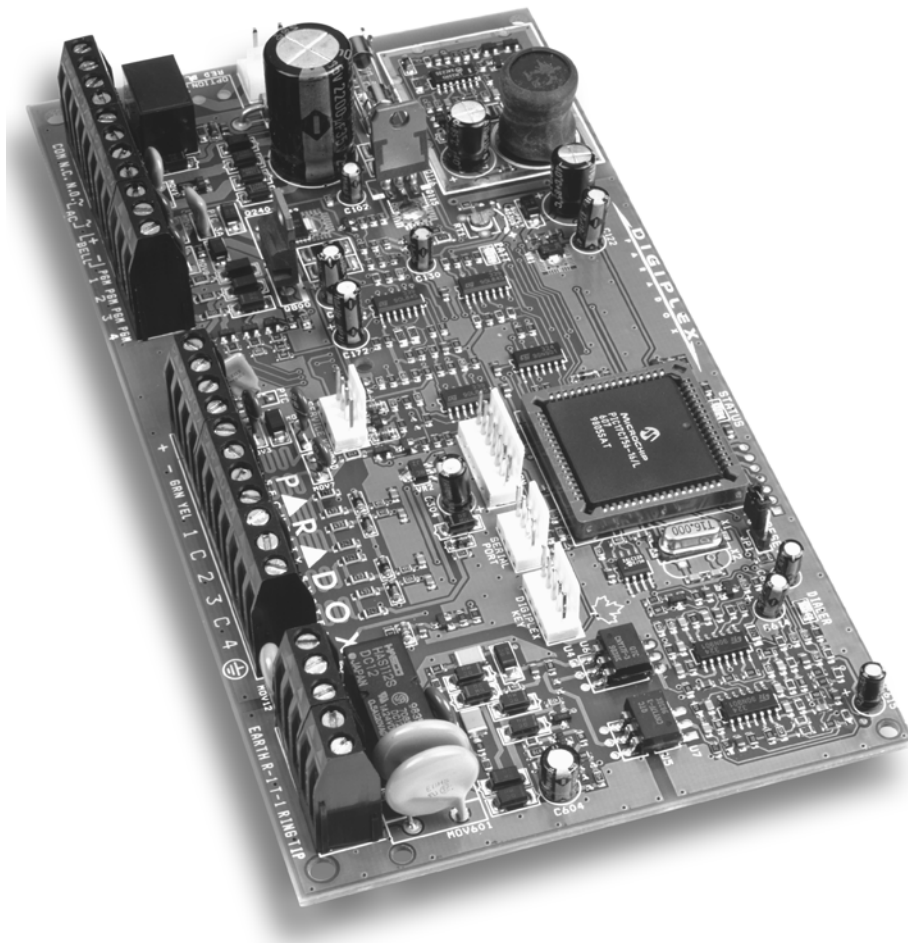


DIGIPLX™



CE FC IC

Digiplex Control Panel - V3.0



DGP-48

Reference and Installation Manual

P ▲ R ▲ D O X®
S E C U R I T Y S Y S T E M S

TABLE OF CONTENTS

INTRODUCTION	4
1.1 Features	4
1.2 Specifications	4
INSTALLATION	5
2.1 Location & Mounting	5
2.2 Earth Ground	5
2.3 AC Power	5
2.4 Backup Battery	5
2.5 Auxiliary Power Terminals	5
2.6 Telephone Line Connection	5
2.7 Bell/siren Output	5
2.8 Calculating Power Requirements	7
2.9 Programmable Outputs	9
2.10 Network Connections	9
2.11 Single Zone Connections	9
2.12 Double Zone Connections	10
2.13 Keypad Zone Connections	10
2.14 Keyswitch Connections	10
2.15 Fire Circuits	10
2.16 Connecting the DGP2-ZX4	11
PROGRAMMING METHODS.....	12
3.1 Panel Programming Mode	12
3.2 Module Programming Mode	12
3.3 Feature Select Programming	12
3.4 Decimal Programming	12
3.5 Hexadecimal Programming	12
3.6 Level Programming	12
3.7 Paradox Memory Key	13
ZONE PROGRAMMING.....	14
4.1 Zone Numbering	15
4.2 Zone Definitions	15
4.3 Zone Partition Assignment	16
4.4 Zone Options	16
4.5 Input Speed	17
4.6 EOL Zones	17
4.7 Zone Doubling (ATZ)	17
KEYSWITCH PROGRAMMING	18
5.1 Keyswitch Numbering	18
5.2 Keyswitch Definitions	19
5.3 Keyswitch Partition Assignment	19
5.4 Keyswitch Options	19
ARMING & DISARMING OPTIONS	20
6.1 Arming Follows Partition	20
6.2 No Arming On Battery Fail	20
6.3 No Arming On Tamper	20
6.4 No Arming On Supervision Loss	20
6.5 Timed Auto-Arming	20
6.6 No Movement Auto-Arming	20
6.7 Auto-Arming Options	21
6.8 One-touch Features	21
6.9 Exit Delay	21
6.10 Keypad Lock-out Feature	21
6.11 Maximum Bypass Entries	22
6.12 Display "Bypass" If Armed	22

6.13 Bell Squawk	22
6.14 Ring-back	22
6.15 Switch To Stay Arming	22
ALARM OPTIONS	23
7.1 Bell/alarm Output	23
7.2 Bell Cut-off Timer	23
7.3 Wireless Transmitter Supervision Options	23
7.4 Tamper Recognition Options	23
7.5 Keypad Panic Options	24
EVENT REPORTING	25
8.1 Reporting Enabled	26
8.2 Report Codes	26
8.3 Central Station Phone #	28
8.4 Partition Account #	28
8.5 Reporting Formats	28
8.6 Event Call Direction	29
8.7 Recent Close Delay	29
8.8 Auto Test Report	29
8.9 Power Fail Report Delay	29
8.10 Disarm Reporting Options	29
8.11 Zone Restore Report Options	29
8.12 Pager Delay	29
8.13 Auto Report Code Programming	30
DIALER OPTIONS.....	31
9.1 Telephone Line Monitoring	31
9.2 Tone/pulse Dialing	31
9.3 Pulse Ratio	31
9.4 Busy Tone Detection	31
9.5 Switch To Pulse	31
9.6 Bell On Communication Fail	31
9.7 Dial Tone Delay	31
PROGRAMMABLE OUTPUTS.....	32
10.1 PGM Activation Event	32
10.2 PGM Deactivation Option	32
10.3 PGM1 Is Smoke Input	33
PGM PROGRAMMING TABLE	34
SYSTEM SETTINGS & COMMANDS	37
12.1 Hardware Reset	37
12.2 Software Reset	37
12.3 Battery Charge Current	37
12.4 Installer Code Lock	37
12.5 Partitioning	37
12.6 Installer Function Keys	37
12.7 System Date & Time	38
12.8 Shabbat Feature	38
12.9 Module Reset	38
12.10 Locate Module	38
12.11 Module Programming	38
12.12 Module Broadcast	38
12.13 Remove Module	38
12.14 Serial Number Viewing	38
12.15 Power Save Mode	39
12.16 Auto Trouble Shutdown	39
12.17 No AC Fail Display	39

ACCESS CODES	40
13.1 Installer Code	40
13.2 Access Code Length	40
13.3 System Master Code	40
13.4 Programming Access Codes	40
13.5 User Options	41
13.6 User Partition Assignment	41
13.7 Access Control	41
13.8 Multiple Action Feature	42
ACCESS CONTROL	43
14.1 Programming Access Control Overview	43
14.2 Common Access Control Terms	43
14.3 Enable Access Control	43
14.4 Assigning The Keypad To A Door	43
14.5 Door Access Mode	43
14.6 Access Levels	44
14.7 Schedules	44
14.8 Holiday Programming	44
14.9 Logging Access Control Events	44
14.10 Global Access Door Features	45
WINLOAD SOFTWARE	46
15.1 Answering Machine Override	46
15.2 Ring Counter	46
15.3 Panel Identifier	46
15.4 PC Password	46
15.5 PC Telephone Number	46
15.6 Call WinLoad	46
15.7 Answer WinLoad	46
15.8 Event Buffer Transmission	46
15.9 Call Back Feature	46
USER FEATURES	47
16.1 Arming and Disarming Features	47
16.2 Bypass Programming	47
16.3 Chime Zones	48
16.4 Access Codes	48
16.5 Normal and Confidential Modes	48
16.6 Keypad Settings	48
16.7 Trouble Display	49
16.8 Event Record Display	50
INDEX.....	51
WARNINGS	56
WARRANTY	57

INTRODUCTION

Paradox Security Systems has once again redefined the boundaries of the security industry and is proud to introduce the Digiplex Control Panel. A new generation in control panel technology, the Digiplex Control Panel uses a quad-wire communication network that provides power and two-way communication for up to 95 modules (keypads, motion detectors, expansion modules, etc.). This, combined with four true partitions, event call direction and the zone numbering feature, simplifies the task of installing or making changes to your security system. The innovative new programming method makes programming the control panel logical and much simpler to execute. This new generation of control panels offers increased capabilities with countless new features without compromising its user-friendliness. If anything, these new control panels are easier to use and easier to install, making the Digiplex Control Panel the ultimate in reliable security protection.

CTR-21 APPROVAL

The Digiplex DGP-48 control panel meets the European Union Common Technical Requirement CTR-21. The CTR-21 requirement is an electrical standard that defines the analogue interface for all two-wire telecommunications equipment (i.e. DECT, PABXs, etc.) intended for connection to the Public Switched Telephone Network. This allows the Digiplex control panel to be used in as many as 19 countries such as Belgium, Germany, Greece, Portugal, Sweden and Switzerland. Uploading or downloading with the WinLoad Security System Management Software is up to 30% faster due to some of the changes required for CTR-21 approval. Digiplex control panels with the CTR-21 approval are available as an option only (order number DGP-48CTR).

1.1 FEATURES

- Digital multiplexed system
- Digital, four-wire communication network:
 - ◆ Provides power and two-way communication to all modules connected to the network.
 - ◆ one network for up to 95 modules
 - ◆ All modules have Plug and Play capability
 - ◆ Connect modules up to 3000ft (914m) from the panel.
 - ◆ Full supervision and sabotage-proof technology without additional wiring
- Up to 48 addressable zones
- 8 independent keyswitch zones (does not use any of the 48 zones)
- 4 on-board hardwired input terminals
- 4 True Partitions:

Most features and options in the Digiplex System can be independently set for each partition such as event reporting, entry/exit delay, bell squawk, quick arming, panics and many more. All zones, keyswitches, user codes and keypads are assigned to specific partitions, making this a true partitioned system.
- 95 User Codes, 1 Installer and 1 System Master
- Up to 4 fully programmable outputs (PGMs) are available. PGM1 can be set as a two-wire smoke detector input. Optional 5A relay also available.
- Simple, direct and logical programming
- Event Call Direction:

The Digiplex Control Panel events are divided into three event groups for each partition and two system event groups. Each event group can be programmed with a separate dialing sequence for each partition.

- 4 Central Station Telephone Numbers
- SIA, Contact ID, Pager Format and many more Communicator Formats
- Remote and local programming of all modules
- Upload/download capability using new WinLoad Security System Management software for Windows®.
- Addressable PIRs and door contacts
- And much, much, more...

1.2 SPECIFICATIONS

CONTROL PANEL

- AC Power: 16VAC, 20/40VA, 50-60Hz
- Battery: 12VDC, 4Ah minimum
- Aux. Power: 12VDC 600mA typical, 700mA maximum, fuseless shutdown at 1.1A
- Bell Output: 1A, fuseless shutdown @ 3A
- PGM Output: PGM1 (100mA), PGM2 - PGM4 (50mA) and PGM5 (5A optional relay)
- Event Buffer: 1024 events
- All control panel outputs are rated to operate between 10.8Vdc and 12.1Vdc

INSTALLATION

2.1 LOCATION & MOUNTING

Before mounting the cabinet, push the five white nylon mounting studs into the back of the cabinet. Pull all cables into the cabinet and prepare them for connection before mounting the circuit board into the back of the cabinet. Select an installation site that is not easily accessible to intruders and leave at least 2" around the panel box to permit adequate ventilation and heat dissipation. The installation site should be dry and close to an AC source, ground connection and telephone line connection.

2.2 EARTH GROUND

Connect the zone and dialer ground terminals from the control panel to the cabinet and cold water pipe or grounding rod as per local electrical codes.



For maximum lightning protection, use separate earth grounds for the zone and dialer grounds as shown in Figure 2-3 on page 6.

2.3 AC POWER

Use a 16.5VAC (50/60Hz) transformer with a minimum 20VA rating to provide sufficient AC power. For increased power you can use a transformer with a 40VA rating. *For UL Listed systems, you can use model #BE156240CAA. For CSA listed systems, use model #BE116240AAA.* Do not use any switch-controlled outlets to power the transformer. Connect the transformer as shown in Figure 2-3 on page 6.



During power up, the control panel will begin a module scan (see section 12.6) that will last between 30 and 120 seconds.



Do not connect the transformer or the backup battery until all wiring is completed.

2.4 BACKUP BATTERY

In order to provide power during power loss, connect a 12VDC 4Ah/7Ah rechargeable acid/lead or gel cell backup battery (YUASA model #NP7-12 recommended) as shown in Figure 2-3 on page 6. Connect the backup battery after applying AC power. When installing, verify proper polarity, as reversed connections will blow the battery fuse. For information on how to set the Battery Charge Current to either 350mA or 700mA, please refer to section 12.3 of this manual.

2.4.1 Battery Test

The control panel conducts a dynamic battery test under load every 64 seconds. If the battery is disconnected, if its capacity is too low or if the battery voltage drops to 10.5 volts or less when there is no AC, the "Battery Trouble" message will appear in the Trouble Display. At 8.5 volts, the panel shuts down and all outputs close.

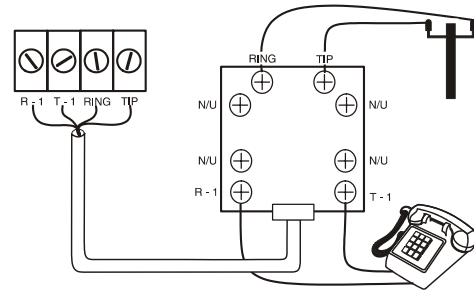
2.5 AUXILIARY POWER TERMINALS

You can use the auxiliary power supply to power the motion detectors, keypads and other accessories in your security system. A fuseless circuit protects the auxiliary output against current overload and automatically shuts down if the current exceeds 1.1A. Auxiliary power will resume once the overload condition has restored. For details on available output power, please refer to Figure 2-3 on page 6. For more information on how to calculate system consumption, refer to "Calculating Power Requirements" on page 7..

2.6 TELEPHONE LINE CONNECTION

Connect the incoming telephone company wires into the TIP and RING connections of the control panel. Then run the wires from T1 and R1 to the telephone system as shown in Figure 2-1.

Figure 2-1: Telephone Line Connections



2.7 BELL/SIREN OUTPUT

The BELL+ and BELL- terminals power bells and/or other warning devices that require a steady voltage output during an alarm. The bell output supplies 12VDC upon alarm and can support two 20-watt or two 30-watt sirens. The bell output uses a fuseless circuit and will automatically shut down if the current exceeds 3A. If the load on the BELL terminals returns to normal ($\leq 3A$), the control panel will re-instate power to the BELL terminals. When connecting sirens, please verify correct polarity as shown in Figure 2-2. Please note that PGM5 is rated at 5A and can be used to power bells and/or other warning devices (see Figure 2-2: Bell/Siren) by programming it as a bell/siren output. Please refer to Programmable Outputs in section 10.



When the bell/siren output is not used, the "Bell Absent" message will appear in the Trouble Display. To avoid this, connect a 1k Ω resistor across the bell output.

Figure 2-2: Bell/Siren

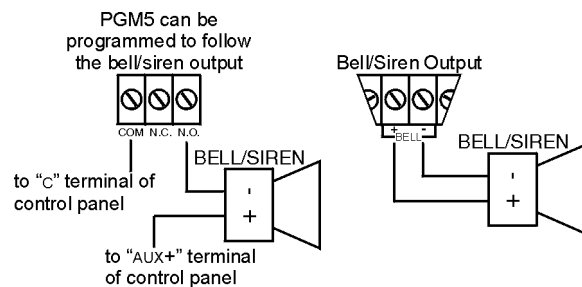
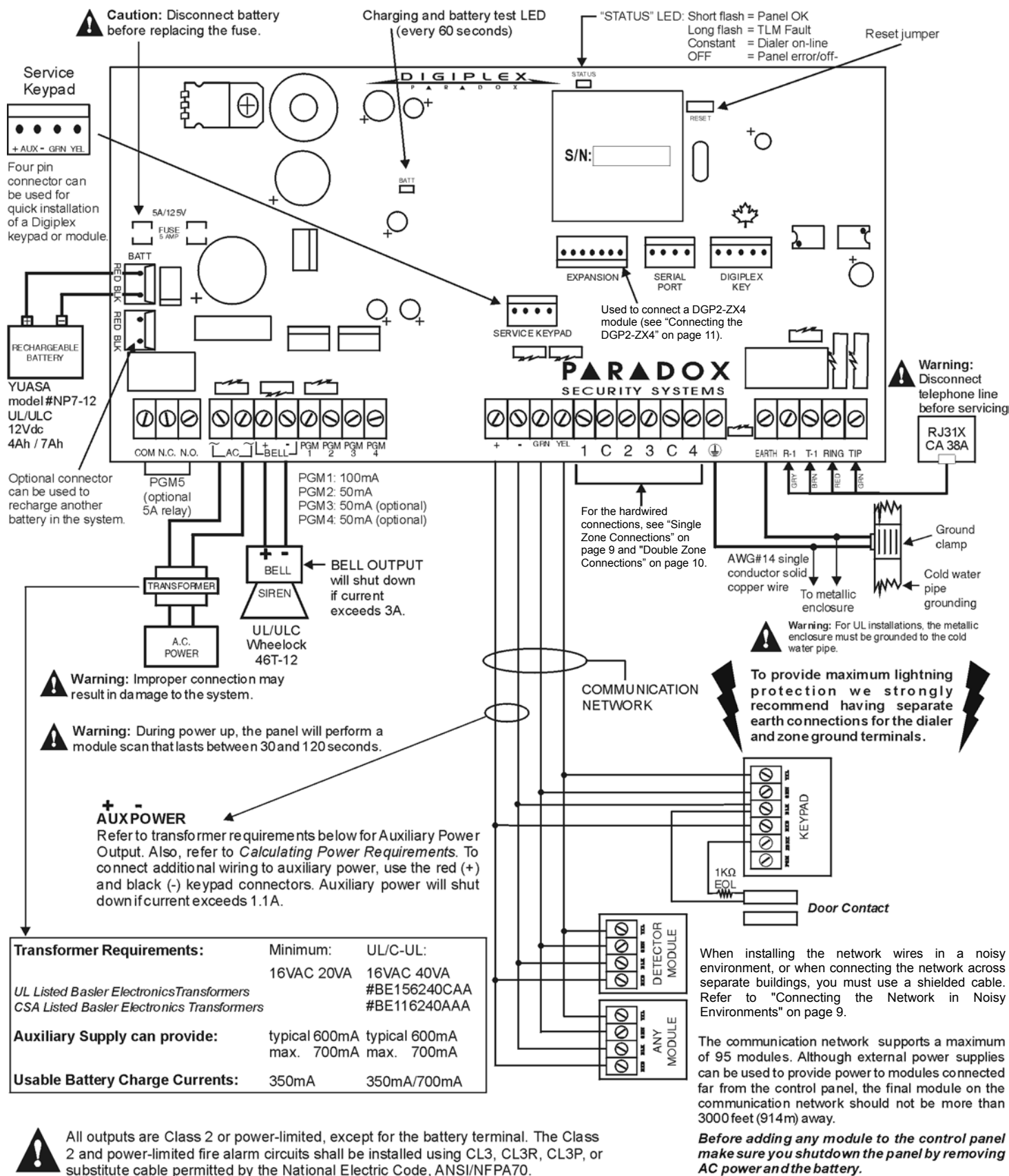


Figure 2-3: Digiplex Control Panel PCB Layout



2.8 CALCULATING POWER REQUIREMENTS

Table 1: Power Unit Consumption Table

Description	QTY.	PU used by each	Total PU
LCD Keypads (DGP2-641):	_____	X 80PU =	_____ PU
Access Control LCD Keypads (DGP2-641AC):	_____	X 150PU =	_____ PU
LED Keypads (DGP-620/648):	_____	X 45PU =	_____ PU
Addressable Digital Motion Detectors (DGP2-50/60/70):	_____	X 25PU =	_____ PU
Addressable Door Contacts (DGP2-ZC1)	_____	X 14PU =	_____ PU
1-Zone Hardwire Modules (DGP2-ZX1)	_____	X 25PU =	_____ PU
4-Zone Hardwire Modules (APR3-ZX4)	_____	X 20PU =	_____ PU
8-Zone Hardwire Modules (APR3-ZX8)	_____	X 40PU =	_____ PU
Omnia Wireless Modules (OMN-RCV3):	_____	X 50PU =	_____ PU
900MHz Wireless Modules (DGP-319):	_____	X 70PU =	_____ PU
1-PGM Output Module (APR3-PGM1):	_____	X 25PU =	_____ PU
4-PGM Output Module (APR3-PGM4):	_____	X 150PU =	_____ PU
Printer Module (APR3-PRT1)	_____	X 40PU =	_____ PU
InTouch Voice-Assisted Arm/Disarm Module (APR3-ADM2)	_____	X 70PU =	_____ PU
Note: The DGP2-ACM1P consumes 165PU from its own power supply.			
Other devices such as hardwired motion detectors (1mA = 1PU)	_____		_____ PU
Maximum available power units = 700PU		GRAND TOTAL	_____ PU

STEP 1: Using Table 1, calculate the total number of power units (PU) required by each device, module, and accessory in the system. Please take into account devices connected to the control panel's PGM outputs. Since the BELL output has its own power supply, do not include the sirens connected to it in the calculation

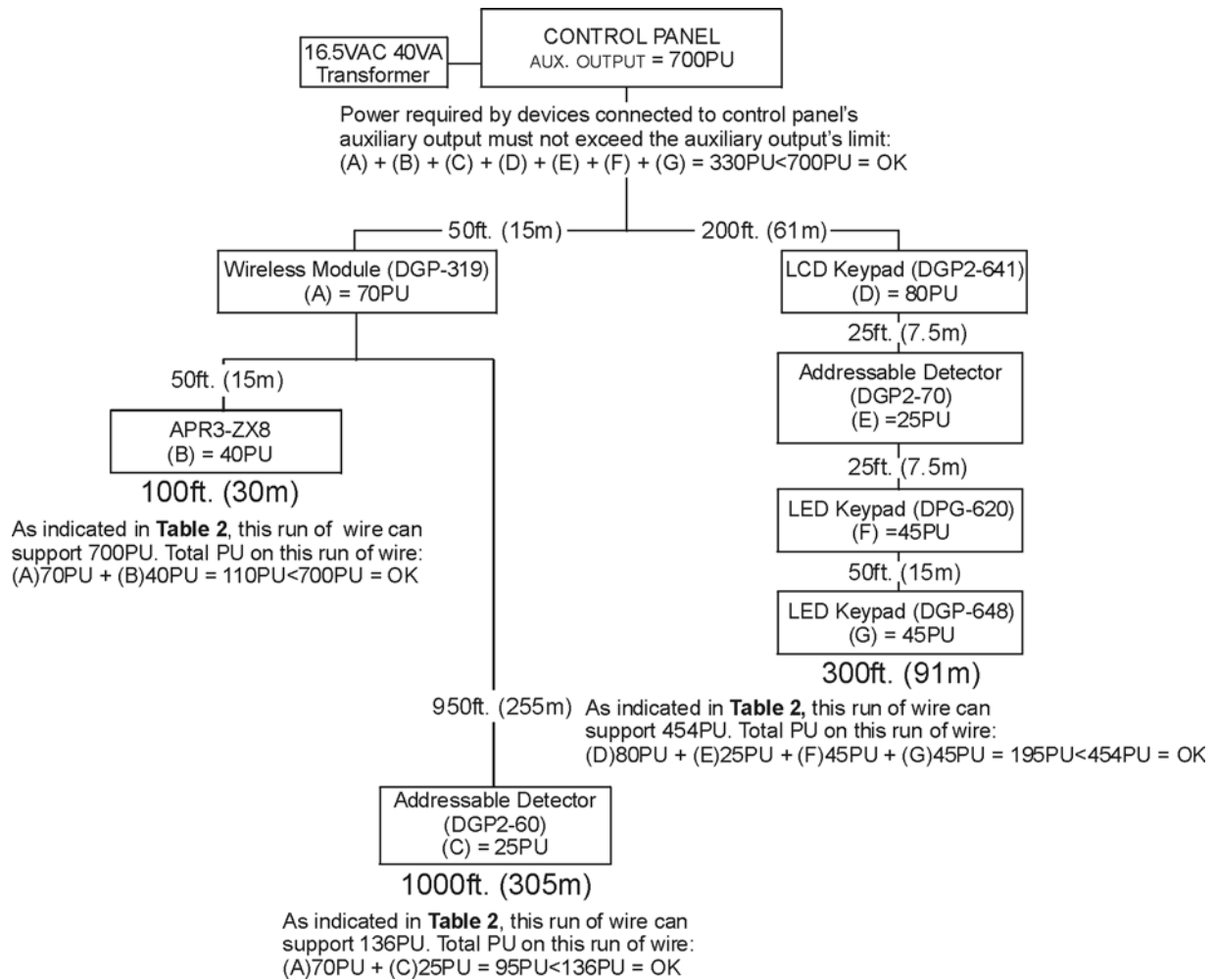
STEP 2: If the value recorded in box "A" is less than 700PU, go to step 3. If the value is greater, you will require an external power supply (see Figure 2-5 on page 8) to provide the additional power needed. Proceed with step 3 and refer to the example in Figure 2-4 on page 8.

STEP 3: Due to the degradation of a power signal over long distances, **EACH** length or run of wire in the system can support only a specific number of power units (PU). Using Table 2: *Power Unit (PU) Limitations For Each Run of Wire*, determine how many power units each length of wire can support. Please note that the total number of power units (PU) can never surpass 700PU.

Table 2: Power Unit (PU) Limitations For Each Run of Wire

Gauge: 18AWG, Surface: 0.823mm ²		Gauge: 22AWG, Surface: 0.326mm ²		Gauge: 24AWG, Surface: 0.205mm ²	
Length of each run of wire	Available Power Units (PU)	Length of each run of wire	Available Power Units (PU)	Length of each run of wire	Available Power Units (PU)
100ft. (30m)	700	100ft. (30m)	700	100ft. (30m)	700
200ft. (61m)	700	200ft. (61m)	682	200ft. (61m)	429
300ft. (91m)	700	300ft. (91m)	454	300ft. (91m)	286
400ft. (122m)	700	400ft. (122m)	341	400ft. (122m)	214
500ft. (152m)	690	500ft. (152m)	273	500ft. (152m)	171
600ft. (183m)	575	600ft. (183m)	227	600ft. (183m)	143
700ft. (213m)	493	700ft. (213m)	195		
800ft. (244m)	431	800ft. (244m)	170		
900ft. (274m)	383	900ft. (274m)	151		
1000ft. (305m)	345	1000ft. (305m)	136		
1500ft. (457m)	230				
2000ft. (610m)	172				
2500ft. (762m)	138				
3000ft. (914m)	115				

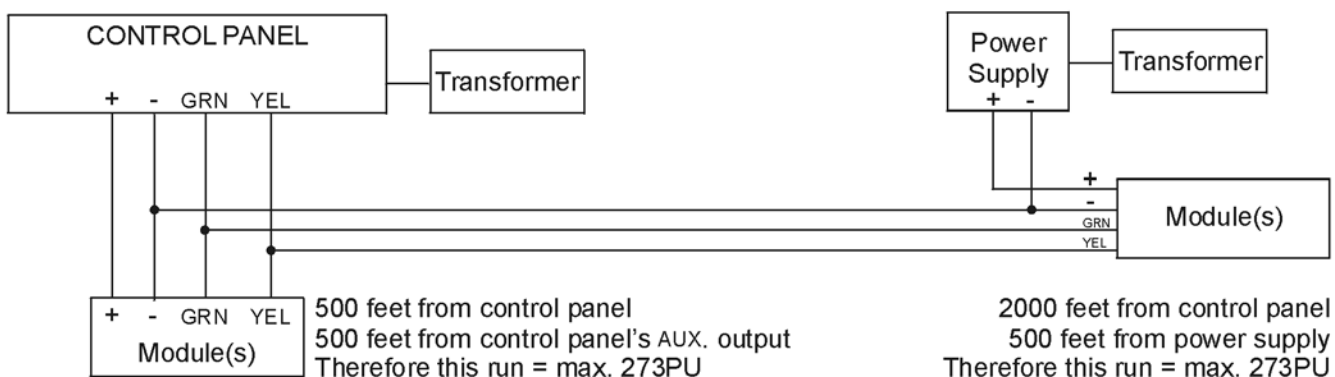
Figure 2-4: Sample Power Requirement Calculations



If in the above example you were to add an LCD Keypad (80PU) to the 100 foot or 300 foot wire, you would not exceed the wire's limit. Although, adding the LCD Keypad to the 1,000 foot wire would exceed the wire's limits, thereby causing devices to function at decreased capacity.

Figure 2-5: External Power Supply Connections

Power units required by devices connected to a power supply do not draw power from the control panel's auxiliary output.



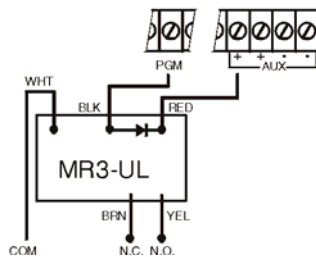
Do not use the same transformer for the control panel and the external power supplies. Modules should never be installed more than 3,000 feet (914m) from the control panel.

2.9 PROGRAMMABLE OUTPUTS

The Digiplex Control Panel comes standard with PGM1 and PGM2. PGM3 to PGM5 are optional. When a specific event or condition occurs in the system, a PGM can be programmed to reset smoke detectors, activate strobe lights, open/close garage doors and much more. For details on how to program the PGMs, refer to section 10.

PGM1 provides a maximum 100mA output, PGM2 to PGM4 provide a maximum 50mA output and PGM5 is a relay output that provides a maximum of 5A. If the current draw on the PGM is to exceed the current output, we recommend the use of a relay as shown in Figure 2-6. PGM1 to PGM4 are normally open outputs and PGM5 is a normally open or normally closed 5A relay. Also, note that PGM1 can be programmed as a 2-wire smoke detector input. For more information, refer to section 2.15.1 and section 10.3 of this manual.

Figure 2-6: PGM Relay Output



2.10 NETWORK CONNECTIONS

The network is a 4-wire communication network that provides power and two-way communication between the control panel and all modules connected to it. All addressable detection devices, keypads and Digiplex modules are connected to the network, which can support up to 95 modules. Connect the four terminals labeled RED, BLK, GRN and YEL of each detector, keypad or module to the corresponding terminals of the control panel as shown in Figure 2-3 on page 6. Please note that all modules can be connected in a star and/or daisy chain configuration. The final device on the communication network should not be more than 3000ft (914m) from the control panel. For information on how to assign a detection device to a zone in the control panel, please refer to "Zone Programming" on page 14..



Before connecting a module to the control panel, shutdown the control panel by removing AC and battery power.

2.10.1 Connecting the Network in Noisy Environments

When installing the network wires in proximity to high electrical interference such as neon lights, motors, high-voltage wiring, transformers, or when connecting the network across separate buildings, you must use shielded cables. Connect the shielded cable as detailed below:

Within the Same Building: Strip the outer jacket at one end of the shielded cable to expose the shield and connect the shield to the control panel ground (not the dialer ground), while leaving the shield at the other end of the cable open (floating).

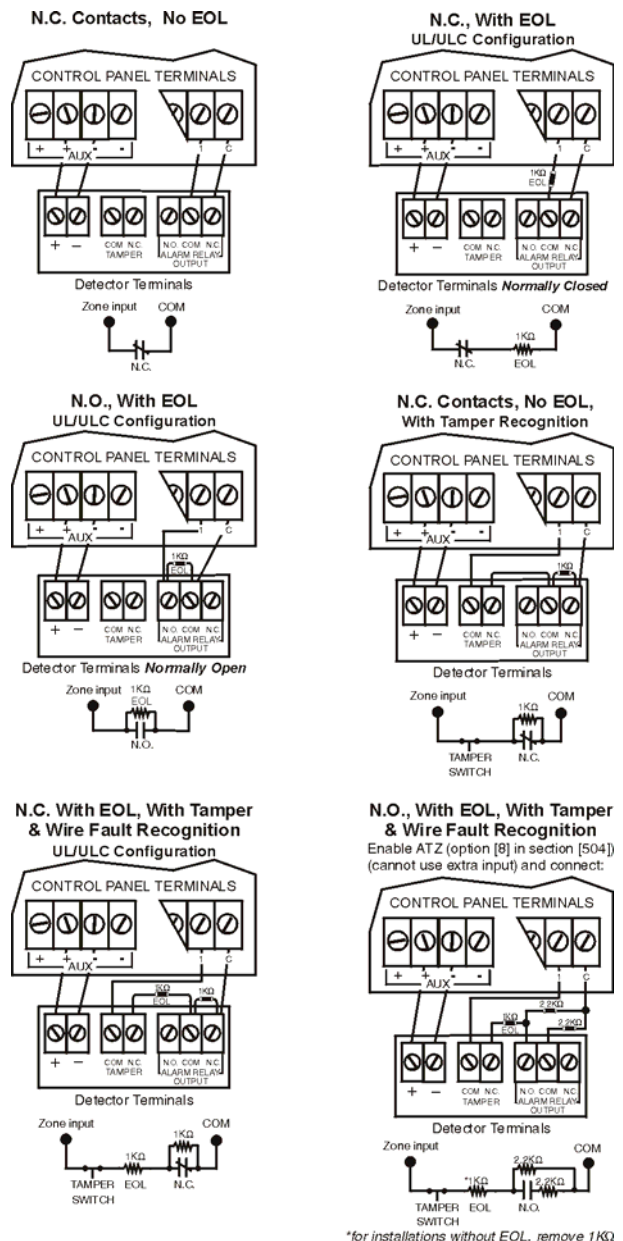
Across Separate Buildings: Strip the outer jacket at one end of the shielded cable to expose the shield. In the same building that houses the control panel, connect the exposed shield to a cold

water pipe or any other earth ground available, while leaving the shield at the other end of the cable open (floating). The same configuration applies for any subsequent building.

2.11 SINGLE ZONE CONNECTIONS

In addition to the network, the Digiplex Control Panel includes four hardwired input terminals for use with traditional hardwired door contacts, smoke detectors and/or motion detectors. The control panel also supports one on-board Expansion Module, the DGP2-ZX4. The DGP2-ZX4 will add four hardwired input terminals to the control panel. One to eight-Zone Expansion Modules that connect to the network are also available. Devices connected to hardwired input terminals must be assigned to a zone and the zone's parameters must be defined. Please refer to "Zone Programming" on page 14. for more information. Figure 2-7 demonstrates single zone (ATZ disabled) hardwire input terminal connections recognized by the Digiplex system. For UL listed installations, use EOL resistor part #2011002000.

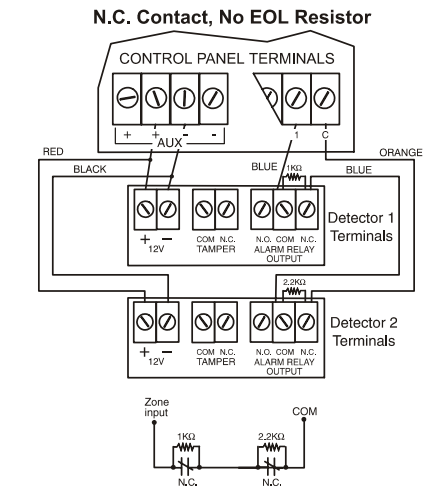
Figure 2-7: Single Zone Input Connections



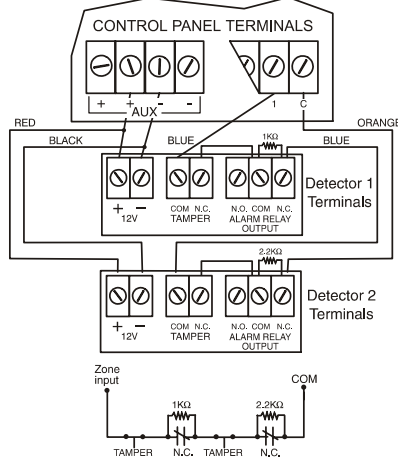
2.12 DOUBLE ZONE CONNECTIONS

Enabling the ATZ feature (see section 4.7) allows you to install two detection devices per input terminal. The ATZ feature is a software oriented feature. Simply connect the devices as shown in Figure 2-8. Devices connected to input terminals must be assigned to a zone and the zone's parameters must be defined. Please refer to "Zone Programming" on page 14. for more information. For UL listed installations, use EOL resistor part #2011002000.

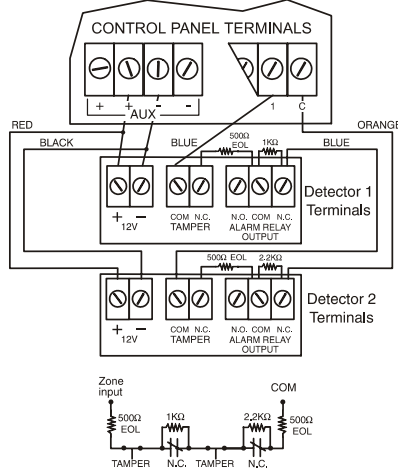
Figure 2-8: Double Zone Connections



N.C. Contact, No EOL, With Tamper Recognition



N.C. Contacts, With EOL, With Tamper & Wire Fault Recognition (UL/ULC)



2.13 KEYPAD ZONE CONNECTIONS

Each keypad has one hardwired input terminal allowing you to connect a detector or door contact directly to the keypad. For example, a door contact located at the entry point of an establishment can be wired directly to the input terminal of the entry point keypad instead of all the way to the control panel.



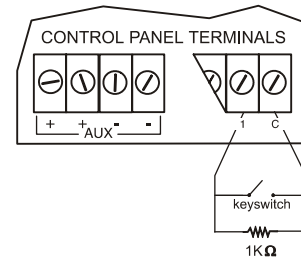
Even with the ATZ feature enabled in the control panel, only one device can be connected to the keypad's hardwired input terminal. Tamper is not recognized on keypad zones. The keypad zone follows the control panel's EOL definition.

A device connected to the keypad's input terminal must be assigned to a zone in the control panel and the zone's parameters must be defined (see "Zone Programming" on page 14.). The keypad will communicate the status of the zone to the control panel via the communication network. The detection device is connected as shown in Figure 2-3 on page 6.

2.14 KEYSWITCH CONNECTIONS

Connect the keyswitches to the keypad, control panel, or Zone Expansion Module's hardwired input terminals as shown in Figure 2-9. Once a keyswitch is connected, it must be assigned a keyswitch zone and its parameters must be defined as described in "Keyswitch Programming" on page 18..

Figure 2-9: Keyswitch Connections



2.15 FIRE CIRCUITS

Connect the smoke detectors used in the security system using any of the following methods. Smoke detectors connected to the control panel or zone expansion input terminals must be assigned to a zone in the control panel and the zone's parameters must be defined as a Fire Zone. For more details, refer to "Zone Programming" on page 14..

2.15.1 Smoke Detector Installation (2-Wire)

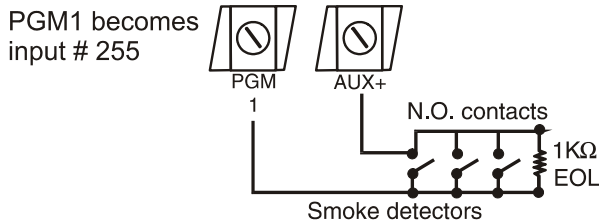
PGM1 can be defined as a 2-wire smoke detector input (see section 10.3) enabling smoke detectors to be connected as shown in Figure 2-10 on page 11. Fire Zones must use a 1kΩ EOL resistor. If there is a line short or if the smoke detector becomes active, whether the system is armed or disarmed, the control panel will generate an alarm. If the line is open, the "Zone Fault" trouble indication will appear in the Trouble Display and will transmit the appropriate report code to the central station (if programmed).

2.15.2 ESL CleanMe™ Installation

The Digiplex control panel supports the use of ESL smoke detectors that have the CleanMe™ feature. The ESL smoke detectors are connected exactly like standard smoke detectors as

shown in Figure 2-10. Please note that you should avoid connecting more than 20 ESL smoke detectors. When an ESL smoke detector sends a CleanMe™ signal, the control panel will generate a Zone Fault trouble and if programmed will transmit the Fire Loop report code to the central station. The trouble will be cleared if there is no CleanMe™ signal for 255 seconds. If an alarm occurs, the trouble will be cleared until it is detected again.

Figure 2-10: PGM1 2-wire Smoke Detector Input



When using ESL smoke detectors with the CleanMe™ feature, do not connect more than 20 detectors in parallel.

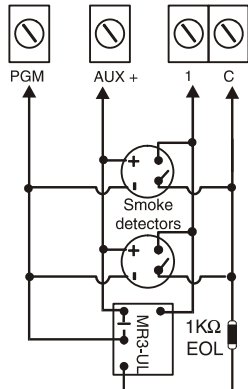
2.15.3 Smoke Detector Installation (4-Wire)

Connect the 4-wire smoke detectors and a relay as shown in Figure 2-11. Recommended: The System Sensor model 2112/24D smoke detectors. To comply with UL955, the 4-wire smoke detectors must be installed using 18 gauge wire. In the event power is interrupted, the relay will cause the control panel to transmit the Fire Loop Trouble report if programmed in section [707]. To reset (unlatch) the smoke detector after an alarm, verify that the negative (-) of the smoke detector is connected to a PGM as shown in Figure 2-11. Then program the PGM with the "Smoke Reset" activation event (see section 10.1 of this manual) to interrupt power to the smoke detector for four seconds when the [CLEAR] and [ENTER] keys are pressed and held for two seconds.

Figure 2-11: Fire Zones

UL/ULC INSTALLATION

CONTROL PANEL TERMINALS



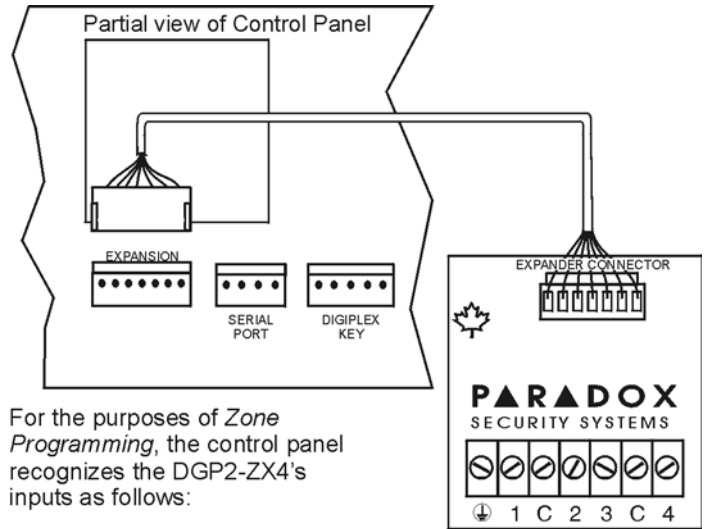
SINGLE FIRE ZONE CONNECTIONS ONLY

If the ATZ feature is enabled, do not use the extra input (i.e. in the above example, input 005 cannot be used as a zone).

2.16 CONNECTING THE DGP2-ZX4

The DGP2-ZX4 is a 4-Zone Hardwire Expansion Module that connects directly to the control panel through its on-board EXPANSION connector as shown in Figure 2-12. It provides four additional hardwired input terminals (8 zones with ATZ enabled). Connect detection devices to the DGP2-ZX4's terminals in the same way they are connected to the control panel as shown in Figure 2-7 on page 9 or Figure 2-8 on page 10. Devices connected to hardwired input terminals must be assigned to a zone and the zone's parameters must be defined (see section 4).

Figure 2-12: Connecting the DGP2-ZX4



NO ATZ:

DGP2-ZX4 Input 1 = Input 009
DGP2-ZX4 Input 2 = Input 010
DGP2-ZX4 Input 3 = Input 011
DGP2-ZX4 Input 4 = Input 012

ATZ Enabled:

DGP2-ZX4 Input 1 = Input 009 & 013
DGP2-ZX4 Input 2 = Input 010 & 014
DGP2-ZX4 Input 3 = Input 011 & 015
DGP2-ZX4 Input 4 = Input 012 & 016

PROGRAMMING METHODS

The Digiplex Control Panel can be programmed using the WinLoad software, the Paradox Memory Key, or manually by using a keypad. We highly recommend programming the control panel with WinLoad as it greatly simplifies the process and reduces potential data errors. Please refer to "WINLOAD SOFTWARE" on page 46. for details on how to set up the control panel to function with WinLoad.

You can also copy the programmed contents of one Digiplex control panel into as many Digiplex control panels as you need by using the Paradox Memory Key (see section 3.7). Each control panel is programmed in less than 5 seconds.

Keypads and other modules can also be programmed easily by using Module Broadcast (see section 12.12). Once a module is programmed, its sections can be sent to other similar modules through the network.

3.1 PANEL PROGRAMMING MODE

Use the *Programming Guide* to keep track of which sections were programmed and how. In order to program anything in the Digiplex Control Panel you must enter the programming mode.

TO ENTER CONTROL PANEL PROGRAMMING MODE:

- Step 1: Press and hold **[0]** key
- Step 2: Key in the **[INSTALLER CODE]** (Default is 000000)
- Key in the 3-digit **[SECTION]**
- Step 3: Every feature and or option is programmed into a three-digit section starting at **[001]**.
- Key in required **[DATA]**
- Step 4: The type of data required will be detailed in the *Programming Guide* and/or explained in the appropriate sections of this manual.

After entering the required data, the control panel will save the data and automatically advance to the next section or press the **[ENTER]** key to save whatever data has been entered and automatically advance to the next section. Press the **[CLEAR]** key to revert to the preceding step or to erase the current data entry when you are entering data.

3.2 MODULE PROGRAMMING MODE

All modules connected to the communication network are programmed through any keypad in the system. To do so, simply enter *Module Programming Mode* as shown below.

TO ENTER THE MODULE PROGRAMMING MODE:

- Step 1: Press & hold **[0]** key
- Step 2: Key in **[INSTALLER CODE]** (Default is 000000)
- Step 3: Key in section **[953]**

Step 4: Key in 8-digit **[SERIAL NUMBER]** of the module you wish to program

Key in 3-digit **[SECTION]** and required **[DATA]**

Step 5: Refer to the module's *Programming Guide* or the module's Installation Guide for details.

The control panel will redirect all programming to the selected module. To exit the Module Programming Mode, press the **[CLEAR]** key as many times as needed to return to the desired screen. Please note that a module's serial number can be located on the module's PC board or it may already be recorded in the module's Installation Guide.

3.3 FEATURE SELECT PROGRAMMING

Most of the Digiplex Control Panel options are programmed using the Feature Select Method, where each number from 1 to 8 corresponds to a specific feature or option. Set these options by turning the number corresponding to the feature ON or OFF. The option is considered ON when the number appears within the brackets on the LCD keypad or when the number is illuminated on an LED Keypad. You turn options ON and OFF by pressing the corresponding keys on the keypad. Press the keys as many times as you need to select the desired options and then press **[ENTER]** to save.

3.4 DECIMAL PROGRAMMING

Certain sections may require the entry of a 3-digit decimal value from 000 to 255.

3.5 HEXADECIMAL PROGRAMMING

Certain sections may require the entry of one or more Hexadecimal values from 0 to F. Press:

[0] to [9] = values 0 to 9 respectively

[STAY] key	= A	[DISARM] key	= D
[FORCE] key	= B	[BYP] key	= E
[ARM] key	= C	[MEM] key	= F

3.6 LEVEL PROGRAMMING

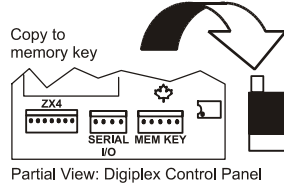
In the sections requiring Level Programming, only one option can be enabled. To enable the option use the **[▲]** and **[▼]** keys. Press **[ENTER]** to save.

3.7 PARADOX MEMORY KEY

Copy the programmed contents of one Digiplex Control Panel into the Paradox Memory Key. Then copy the contents of the Paradox Memory Key into as many Digiplex Control Panels as you need. This saves you a lot of time. All you have to do is program one Digiplex Control Panel, then download the programmed contents to other control panels in less than 5 seconds.

Copy to Memory Key from SOURCE Control Panel

- 1) Remove the AC and battery power from the control panel.
- 2) Place Memory Key on the connector labeled MEM KEY of the control panel that you want to copy. Make sure that the write protect jumper is on.
- 3) Enter section:
[965] to copy the contents of the panel **except sections [001] to [048] (device serial numbers) and [049] to [056] (keyswitch serial numbers)** to the key.
[966] to copy all of the contents including **sections [001] to [048] and [049] to [056]** from the panel to the key.



- 4) When the keypad emits a Confirmation Beep, wait 10 seconds before removing the Memory Key. Remove the jumper if you do not wish to accidentally overwrite the contents of the Memory Key.

Download to DESTINATION Control Panel

- 1) Remove the AC and battery power from the control panel.
- 2) Place the Memory Key on the connector labeled MEM KEY of the control panel that is to receive the contents of the Memory Key.
- 3) Enter section:
[961] to download the contents **except sections [001] to [048] (device serial numbers) and [049] to [056] (keyswitch serial numbers)** from the key to the panel.
[962] to download all of the contents including **sections [001] to [048] and [049] to [056]** from the key to the panel.
- 4) When the keypad emits a Confirmation Beep, wait 10 seconds before removing the Memory Key.

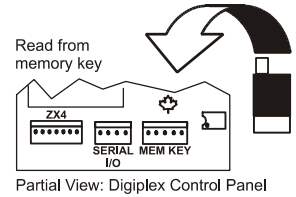
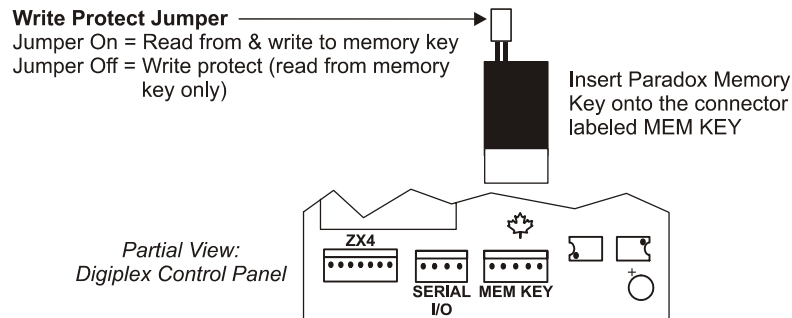


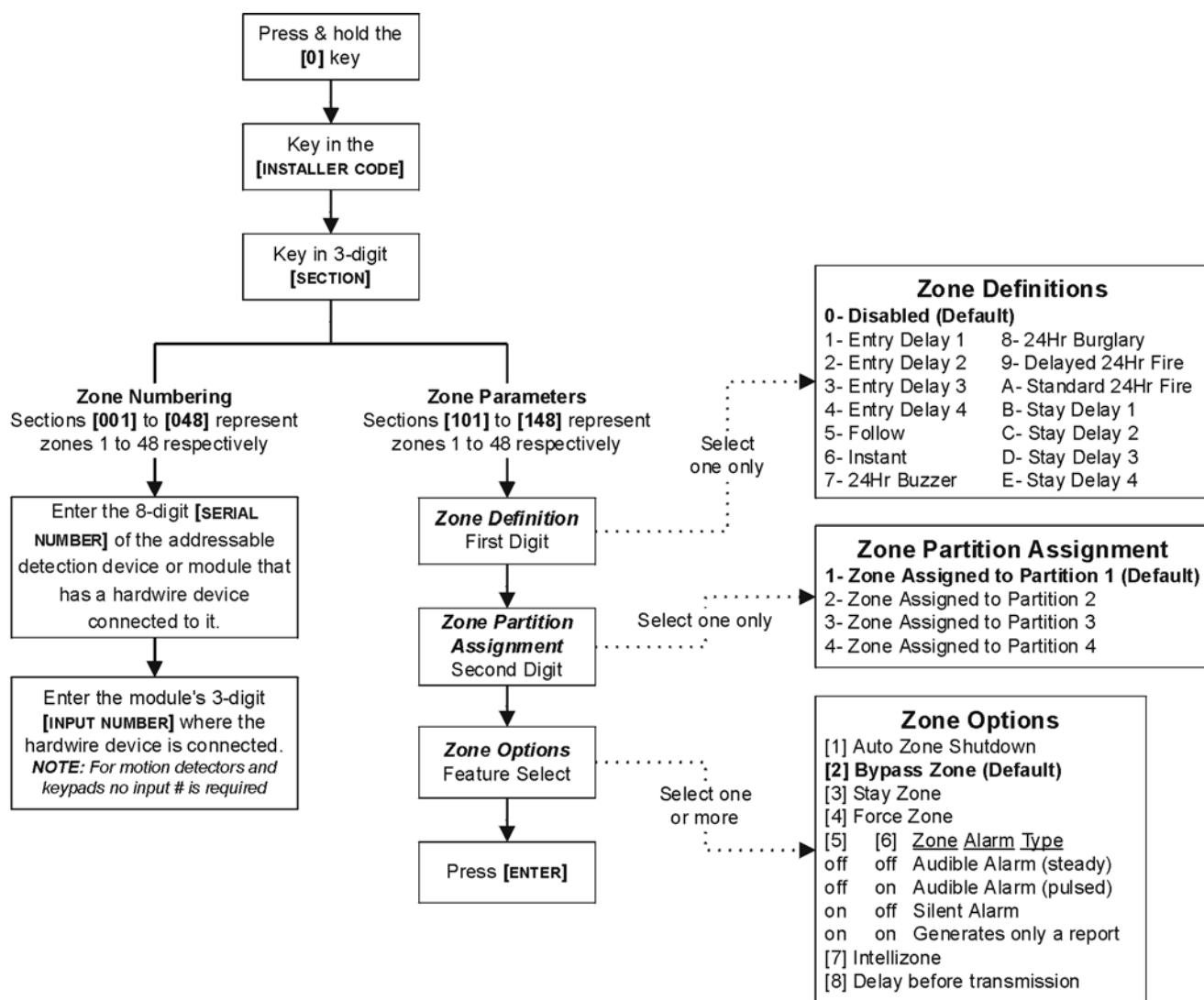
Figure 3-1: Using the Memory Key



- Serial number of the device/module
- Input number of the device/module

- Zone Definition
- Zone Partition Assignment
- Zone Options

to Figure 2-3 on page 6 or to their respective Installation Guides.



4.1 ZONE NUMBERING

SECTIONS [001] TO [048]

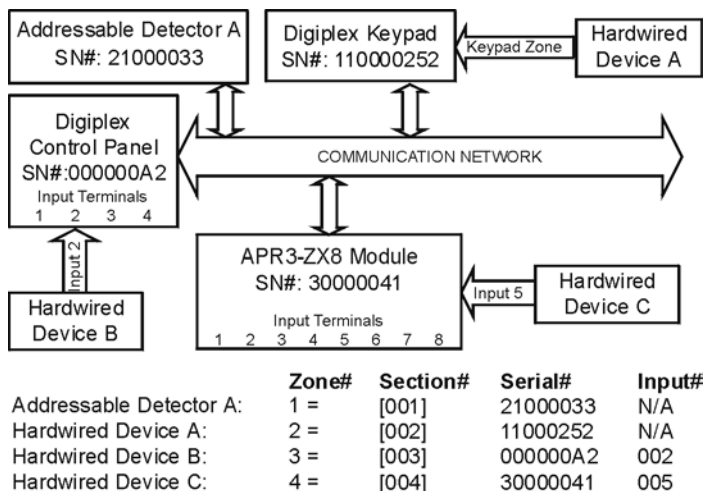
The Zone Numbering feature allows you to assign any detection device in the system to any of the 48 zones. This feature tells the control panel where the device is connected and which of the 48 zones is assigned to that device (see *Figure 4-2: Zone Numbering*).

- To assign an addressable detection device connected to the network, program the detector's serial number into the section corresponding to the desired zone (i.e. program zone 34 in section [034]).
- To assign a detection device connected to a module or control panel's hardwired input terminal, program the module's or control panel's serial number and the input number where the device is connected into the section corresponding to the desired zone. Refer to the appropriate module's Installation Guide for details of its input numbers. Note: an input number is not required for keypad zones.



If PGM1 is defined as a smoke detector input (see section 10.3), the control panel will recognize it as input # 255.

Figure 4-2: Zone Numbering



4.2 ZONE DEFINITIONS

Select one of the 15 available zone definitions described below (also refer to Figure 4-1 on page 14).

4.2.1 Zone Disabled

SECTIONS [101] TO [148]: FIRST DIGIT = 0

Disables the corresponding zone. All zones are disabled by default.

4.2.2 Entry Delays 1 to 4

SECTIONS [101] TO [148]: FIRST DIGIT = 1 TO 4

When an armed zone defined as an Entry Delay opens, the control panel will not generate an alarm until the programmed Entry Delay Timer has elapsed. A zone can be defined with one of four Entry Delays. Each Entry Delay is associated with an Entry Delay Timer.

To program the Entry Delay Timer, key in the desired 3-digit delay value (000 to 255 seconds) into the corresponding section:

- Entry Delay 1 Timer: **[230]**
- Entry Delay 2 Timer: **[231]**
- Entry Delay 3 Timer: **[232]**
- Entry Delay 4 Timer: **[233]**

Please note these are the same timers used for Stay Delay zones (see section 4.2.9). Entry Delay zones are commonly used at the entry/exit points of the protected area (i.e. front/back door or garage). Using different Entry Delays is useful when, for example, one entry point requires a longer delay than the other entry point or in a partitioned system where each partition may require a different Entry Delay.

4.2.3 Follow Zones

SECTIONS [101] TO [148]: FIRST DIGIT = 5

If an armed Follow zone opens, the control panel will immediately generate an alarm. If an armed Entry Delay zone (see section 4.2.2) opens before the Follow zone, the control panel will wait until the end of the Entry Delay before generating an alarm. If more than one Entry Delay zone opens before the Follow zone, the control panel will wait until the end of the first Entry Delay before generating an alarm.

4.2.4 Instant Zones

SECTIONS [101] TO [148]: FIRST DIGIT = 6

When an armed Instant zone opens, the control panel immediately generates an alarm. Instant zones are commonly used for windows, patio doors, skylights and other perimeter type zones.

4.2.5 24Hr Buzzer Zones

SECTIONS [101] TO [148]: FIRST DIGIT = 7

Whenever a 24Hr Buzzer zone opens, whether the zone is armed or disarmed, the control panel will activate the keypad buzzer to indicate that the zone was breached. The control panel will report the alarm, but will not enable the bell/siren output. Enter any valid access code on the keypad to stop the buzzer.



The keypads must be assigned to the same partition as the 24Hr Buzzer zone. Otherwise, the buzzer will not activate.

4.2.6 24Hr Burglary Zones

SECTIONS [101] TO [148]: FIRST DIGIT = 8

Whenever a 24Hr Burglary zone opens, whether the system is armed or disarmed, the control panel will immediately generate an alarm.

4.2.7 Delayed 24Hr Fire Zone

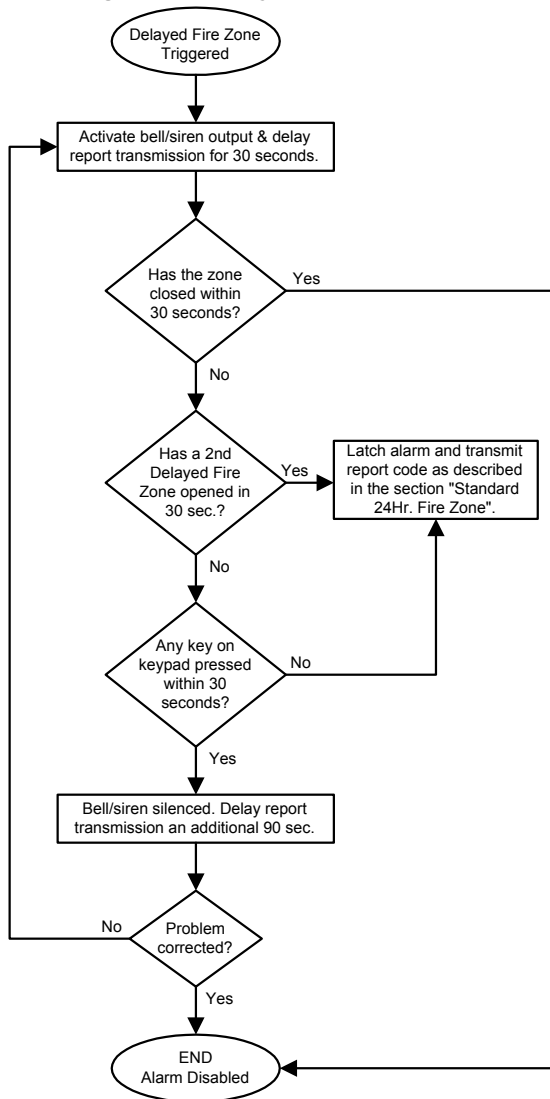
SECTIONS [101] TO [148]: FIRST DIGIT = 9

The Delayed 24Hr Fire Zone definition described in Figure 4-3 on page 16 is commonly used in residential homes where a smoke detector often generates false alarms (i.e. cigarette smoke, burning bread, etc.). When a zone is programmed as a Fire zone, the zone becomes normally open and requires an EOL resistor. The zone will not function as normally closed.



The keypads must be assigned to the same partition as the Delayed 24Hr Fire zone for the buzzer to activate.

Figure 4-3: Delayed 24-hr. Fire Zone



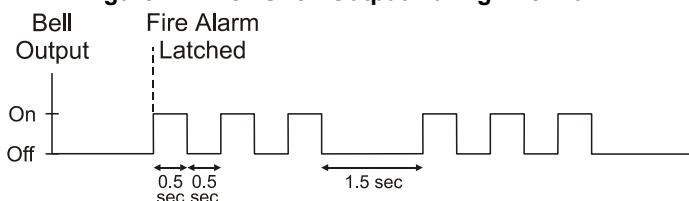
4.2.8 Standard 24Hr Fire Zone

SECTIONS [101] TO [148]: FIRST DIGIT = A

For details how to connect smoke detectors to the control panel, refer to Fire Circuits in section 2.15. When a zone is programmed as a Fire zone, the zone becomes normally open and requires an EOL resistor. The zone will not function as normally closed. Whenever a Standard 24Hr Fire Zone is triggered, whether it is armed or disarmed, the control panel can:

- send a *Zone Alarm* report code (see section 8.2.5).
- send a *Fire Loop Trouble Report* (see section 8.2.11) if a tamper/wiring fault occurs on a Fire Zone. A "Zone Fault Trouble" will also appear in the keypad's Trouble Display.
- generate a Fire alarm, which is always audible, regardless of other settings. Fire alarms will generate an intermittent bell/siren output signal as demonstrated in Figure 4-4.

Figure 4-4: Bell/Siren Output During Fire Alarm



4.2.9 Stay Delay Zone

SECTIONS [101] TO [148]: FIRST DIGIT = B TO E

When a Stay Delay zone is armed using the Regular or Force arming methods, the control panel will process the zone as an Instant zone (see section 4.2.4). When a Stay Delay zone is armed using the Stay or Instant arming methods and the zone is triggered, the control panel will not generate an alarm until the programmed Stay Delay has elapsed. A zone can be defined with one of four Stay Delays. Each Stay Delay is associated with an Entry Delay Timer. To program the Entry Delay Timer, key in the desired 3-digit delay value (000 to 255 seconds) into the corresponding section:
 Stay Delay 1 = Entry Delay 1 Timer in section [230]
 Stay Delay 2 = Entry Delay 2 Timer in section [231]
 Stay Delay 3 = Entry Delay 3 Timer in section [232]
 Stay Delay 4 = Entry Delay 4 Timer in section [233]
 Please note that the Entry Delay Timers are the same timers used for Entry Delay zones.

4.3 ZONE PARTITION ASSIGNMENT

SECTIONS [101] TO [148]: SECOND DIGIT = 1 TO 4

The control panel provides the option of partitioning the security system into two, three, or four completely independent systems. Therefore, each zone must be assigned to one partition as described in Figure 4-1 on page 14. For more information on Partitioning, refer to section 12.5.

4.4 ZONE OPTIONS

Each zone can be programmed with one or more of the options described below. Program the zone options as described in Figure 4-1 on page 14.

4.4.1 Auto Zone Shutdown

SECTIONS [101] TO [148]: OPTION [1]

When option [1] is disabled and an armed zone is breached, the control panel generates an alarm: it may send an alarm report (see section 8.11), activate the bell output, etc.. If the same zone re-opens during the same alarm, another alarm report may be sent, the bell output may re-activate and so on. When option [1] is enabled on a zone, the control panel will stop generating an alarm when the Auto Zone Shutdown Limit is reached during one armed period. The control panel will ignore zones with the Auto Zone Shutdown option that have surpassed the programmed limit. To program the Auto Zone Shutdown Limit, key in the desired 3-digit counter (000 to 015) into section [217]. Entering 000 disables this feature. The Auto Zone Shutdown Limit resets every time the system is armed.

4.4.2 Bypass Zones

SECTIONS [101] TO [148]: OPTION [2]

Only zones with option [2] enabled can be Manually Bypassed (see section 13.5.3). Fire Zones cannot be bypassed. All zones are set as Bypass Zones by default.

4.4.3 Stay Zones

SECTIONS [101] TO [148]: OPTION [3]

Only zones with option [3] enabled will be bypassed when the system is Stay Armed (see section 16.1.2). All other zones will remain activated. Fire Zones cannot be set as Stay Zones.

4.4.4 Force Zones

SECTIONS [101] TO [148]: OPTION [4]

Only zones with option [4] enabled can be bypassed when the system is Force armed (see section 16.1.6). Fire Zones cannot be set as Force Zones.

4.4.5 Alarm Types

SECTIONS [101] TO [148]: OPTIONS [5] & [6]

[5]	[6]	Zone Alarm Type
Off	Off	Steady Audible Alarm
Off	On	Pulsed Audible Alarm
On	Off	Silent Alarm
On	On	Generates a report only

- A *Steady Audible Alarm* transmits the appropriate report code (if programmed) and generates an alarm providing a steady output for any bells or sirens connected to the control panel.
- A *Pulsed Audible Alarm* transmits the appropriate report code and generates an alarm providing a pulsed output (see Figure 4-4 on page 16) for any bells or sirens connected to the panel.
- A *Silent Alarm* transmits the appropriate report code and generates an alarm without activating any bells or sirens (e.g. keypad indicates an alarm and the system must be disarmed).
- A *Report Only* sends the report code to the central station. Unlike a silent alarm, no access codes are required to cancel the alarm. Fire Zones cannot be set to *Report Only*.

4.4.6 Intellizone

SECTIONS [101] TO [148]: OPTION [7]

If an alarm condition occurs on a zone with option [7] enabled, the control panel will trigger the Intellizone Delay and will seek confirmation of the alarm before generating an alarm. An alarm will only be generated if one of the following conditions occurs during the Intellizone Delay:

- 1) An alarm condition occurs on any another Intellizone during the Intellizone Delay.
- 2) The zone in alarm has restored and re-occurred during the Intellizone Delay.
- 3) The zone in alarm remains in alarm for the entire Intellizone Delay.

To program the Intellizone Delay, key in the desired 3-digit delay value (010 to 255 seconds) into section [200]. Fire Zones cannot be set as Intellizones.

4.4.7 Delay Alarm Transmission

SECTIONS [101] TO [148]: OPTION [8]

When an alarm condition occurs on a zone with option [8] enabled, the control panel will generate an alarm, but will not report the alarm to the central station until the end of the Alarm Transmission Delay. During this period, disarming the system will cancel any report originating from this zone. To program the Alarm Transmission Delay, key in the desired 3-digit delay value (001 to 255 seconds, 000 = instant) into section [256]. This feature is commonly used with Entry Delay zones in order to reduce the occurrence of false alarms created by new users who may not disarm the system in time.

4.5 INPUT SPEED

SECTIONS [201] TO [216]

(000 to 255 X 20msec, default: 600ms) The Input Speed defines how quickly the control panel will respond to an open zone detected on any hardwired input terminal. The control panel will not display and/or respond to an open zone until the programmed Input

Speed elapses to prevent glitches from causing an alarm or unnecessary reporting. All other zone definitions and options do not come into effect until the Input Speed has elapsed. The Input Speed does not apply to addressable detection devices. The Input Speed for each input terminal can be set from 20ms to 5.1s, by programming the desired value (001 to 255 X 20ms) into the appropriate section.

Example:

The system is armed and the zone speed is set for 600ms. A zone opens and closes in less than 600ms, the control panel will not respond (i.e. no reporting, no alarm and no display on the keypad).

[201]	Control Panel Terminal 1/ Input 001 speed
[202]	Control Panel Terminal 2/ Input 002 speed
[203]	Control Panel Terminal 3/ Input 003 speed
[204]	Control Panel Terminal 4/ Input 004 speed
[205]	Control Panel Doubler 1/ Input 005 speed
[206]	Control Panel Doubler 2/ Input 006 speed
[207]	Control Panel Doubler 3/ Input 007 speed
[208]	Control Panel Doubler 4/ Input 008 speed

The optional DGP2-ZX4 On-board Zone Expansion (see section 2.16):

[209]	DGP2-ZX4 Terminal 1/ Input 009 speed
[210]	DGP2-ZX4 Terminal 2/ Input 010 speed
[211]	DGP2-ZX4 Terminal 3/ Input 011 speed
[212]	DGP2-ZX4 Terminal 4/ Input 012 speed
[213]	DGP2-ZX4 Doubler 1/ Input 013 speed
[214]	DGP2-ZX4 Doubler 2/ Input 014 speed
[215]	DGP2-ZX4 Doubler 3/ Input 015 speed
[216]	DGP2-ZX4 Doubler 4/ Input 016 speed

4.6 EOL ZONES

SECTION [504]: OPTION [7]

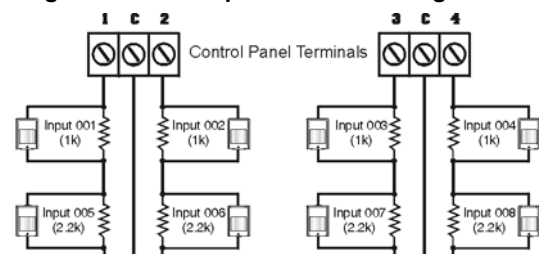
If detection devices connected to hardwired input terminals use 1k Ω end of line resistors, enable option [7] in section [504]. For more information on the use of EOL resistors, refer to Zone Connections in section 2.11 & section 2.12.

4.7 ZONE DOUBLING (ATZ)

SECTION [504]: OPTION [8]

Enabling the ATZ feature allows you to install two detection devices per hardwired input terminal. Each detection device will have its own zone, display its zone status on the keypad and send separate alarm codes for each zone. The extra zones are recognized as described in Figure 4-5. For information on how to connect the detection devices, please refer to Double Zone Connections in section 2.12. Fire Zones cannot be doubled.

Figure 4-5: ATZ Input Terminal Recognition



For ATZ recognition for the DGP2-ZX4, see *Connecting the DGP2-ZX4*.

KEYSWITCH PROGRAMMING

The Digiplex Control Panel can support up to 8 keyswitch zones in addition to the 48 standard zones. A keyswitch allows a user to arm or disarm a system by pressing a key or by toggling a keyswitch. The keyswitches are connected to the hardwired input terminals of either the Digiplex control panel, zone expansion modules or the keypad. For more information on the installation of keyswitches, please refer to section 2.14. Keyswitches must be assigned to a keyswitch zone and that zone must be defined as described in this section:

Keyswitch Numbering [049] to [056]:

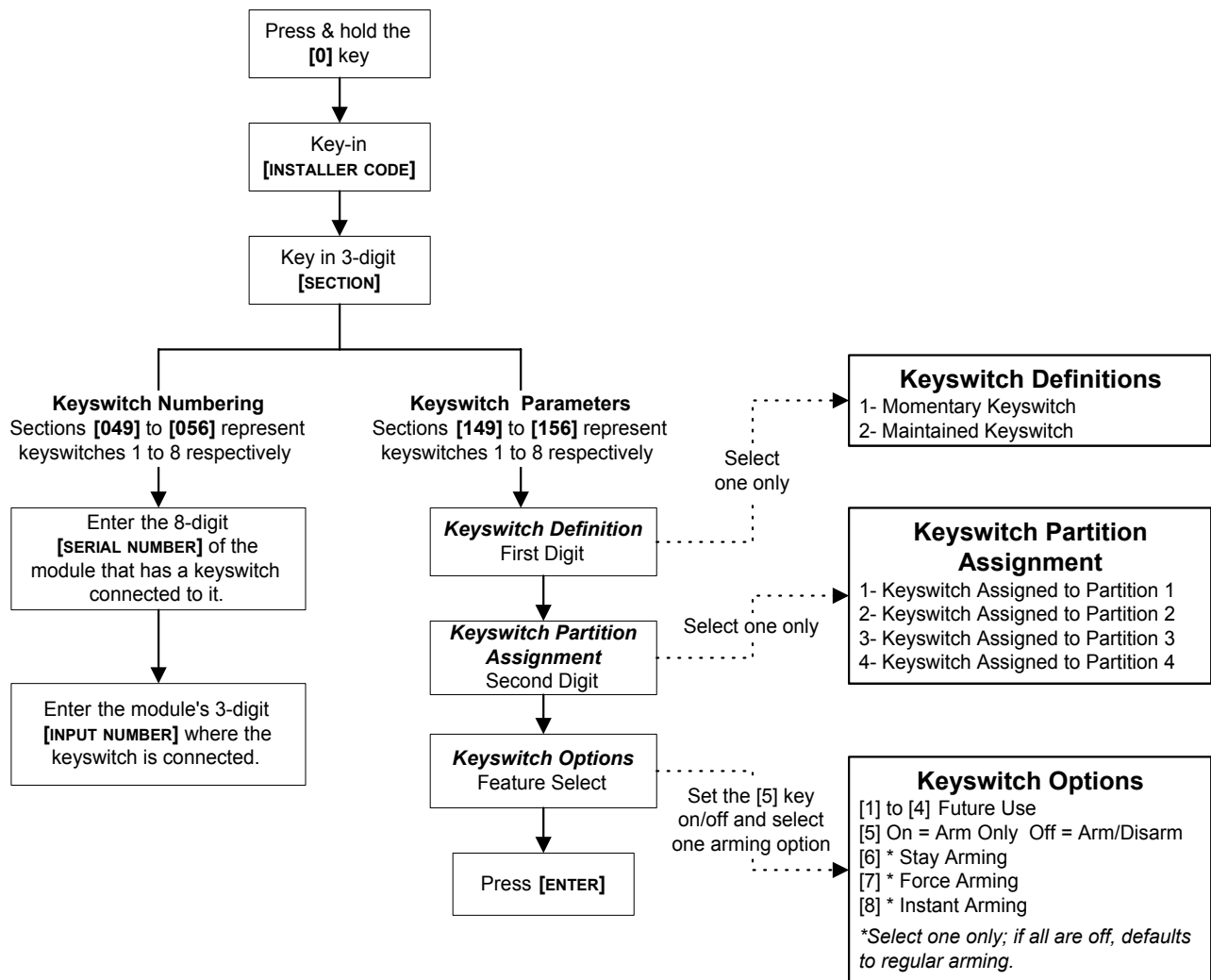
- Serial # of the Module
- Input # of the Module

Keyswitch Parameters [149] to [156]:

- Keyswitch Definitions
- Keyswitch Partition Assignment
- Keyswitch Options

The Keyswitch Numbering feature enables you to individually assign each input to any keyswitch zone in the Digiplex system. Please refer to section 5.1 for details. The Keyswitch Parameters define the keyswitch's partition assignment and its arming method (see section 5.2 to section 5.4).

Figure 5-1: Keyswitch Programming



5.1 KEYSWITCH NUMBERING

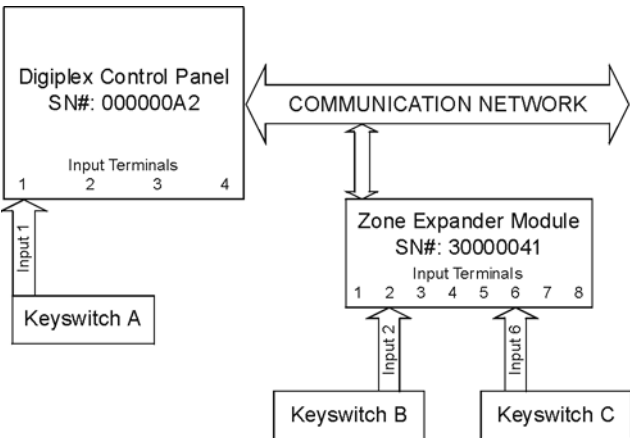
SECTIONS [049] TO [056]

The Keyswitch Numbering feature allows you to assign any hardwired input in the system to any of the 8 keyswitch zones in

the Digiplex Control Panel. This feature tells the control panel where the keyswitch is connected and which of the 8 keyswitch zones is assigned to that keyswitch. To assign a keyswitch connected to a hardwired input terminal, program the module's serial number and the number of the input where the keyswitch is

connected into the section corresponding to the desired keyswitch zone (see Figure 5.2).

Figure 5-2: Example of Keyswitch Numbering



Keyswitch				
	Zone #	Section	Serial#	Input#
Keyswitch A:	1 =	[049]	000000A2	001
Keyswitch B:	2 =	[050]	30000041	002
Keyswitch C:	3 =	[051]	30000041	006

5.2 KEYSWITCH DEFINITIONS

Select one of the keyswitch definitions (also see Figure 5-1 on page 18):

5.2.1 Keyswitch Disabled

SECTIONS [149] TO [156]: FIRST DIGIT = 0
Disables keyswitch input.

5.2.2 Momentary Keyswitch

SECTIONS [149] TO [156]: FIRST DIGIT = 1
To arm a partition using the Momentary Keyswitch, turn on the keyswitch for approximately three seconds then turn it off. Repeating this sequence will disarm the system. The selected Keyswitch Option (see section 5.4) determines the type of arming.

5.2.3 Maintained Keyswitch

SECTIONS [149] TO [156]: FIRST DIGIT = 2
To arm a partition using the Maintained Keyswitch, turn the switch from the ON to the OFF position. To disarm a partition set the keyswitch in the ON position. In the case of an *Arm Only* option, the control panel will not perform any action when the switch is in the ON position. The selected Keyswitch Option (see section 5.4) determines the type of arming.

5.3 KEYSWITCH PARTITION ASSIGNMENT

SECTIONS [149] TO [156]: SECOND DIGIT = 1 TO 4
The control panel provides the option of partitioning the security system into two, three, or four completely independent systems. Therefore, each keyswitch must be assigned to one partition as described in Figure 5-1 on page 18. For more information on Partitioning, refer to section 12.5.

5.4 KEYSWITCH OPTIONS

Each keyswitch zone can be programmed with one or more of the options (also see Figure 5-1 on page 18):

5.4.1 Arm/Disarm Option (Keyswitch)

SECTIONS [149] TO [156]:
Option [5] ON = Arm Only
Option [5] OFF = Arm & Disarm



Only one of the arming options (Stay, Force, Instant and Regular) can be selected.

5.4.2 Stay Arming (Keyswitch)

SECTIONS [149] TO [156]: OPTION [6]
Activating the keyswitch will bypass any zones defined as Stay Zones (see section 4.4.3) in the selected partition. All other zones will remain activated. For more information on Stay Arming, refer to section 16.1.2.

5.4.3 Force Arming (Keyswitch)

SECTIONS [149] TO [156]: OPTION [7]
Activating the keyswitch will arm the selected partition bypassing any open zones defined as Force Zones (see section 4.4.4) at the time of arming. For more information on Force Arming, refer to section 16.1.6.

5.4.4 Instant Arming (Keyswitch)

SECTIONS [149] TO [156]: OPTION [8]
This option is identical to Stay Arming except that all armed zones will become Instant Zones (see section 4.2.4). For more information on Instant Arming, refer to section 16.1.4.

5.4.5 Regular Arming (Keyswitch)

SECTIONS [149] TO [156]: OPTION [6] TO [8]
When options [6] to [8] are off, the keyswitch arming option will default to Regular Arming (see section 16.1.1).

ARMING & DISARMING OPTIONS

6.1 ARMING FOLLOWS PARTITION

SECTIONS [505], [509], [513], [517]: OPTIONS [1] TO [4]

A partition can be set to follow the arming and disarming status of one or more partitions. If a partition is set to follow more than one partition, the partition will arm when all selected partitions are armed. However, the partition will disarm as soon as one of the selected partitions is disarmed. For more details on how these options are programmed, please refer to the *Programming Guide*.

Example:

If options [2] and [3] are on in section [505], Partition 1 will automatically arm whenever partitions 2 and 3 are armed. Partition 1 will disarm when either partition 2 or partition 3 is disarmed.

[505] Partition 1:

Option [2] = Partition 1 arms and disarms with Partition 2
Option [3] = Partition 1 arms and disarms with Partition 3
Option [4] = Partition 1 arms and disarms with Partition 4

[509] Partition 2:

Option [1] = Partition 2 arms and disarms with Partition 1
Option [3] = Partition 2 arms and disarms with Partition 3
Option [4] = Partition 2 arms and disarms with Partition 4

[513] Partition 3:

Option [1] = Partition 3 arms and disarms with Partition 1
Option [2] = Partition 3 arms and disarms with Partition 2
Option [4] = Partition 3 arms and disarms with Partition 4

[517] Partition 4:

Option [1] = Partition 4 arms and disarms with Partition 1
Option [2] = Partition 4 arms and disarms with Partition 2
Option [3] = Partition 4 arms and disarms with Partition 3

6.2 NO ARMING ON BATTERY FAIL

SECTION [503]: OPTION [8]

With option [8] on in section [503], the control panel can restrict arming if the control panel detects a battery loss or if the battery voltage is less than 10.5V. The control panel will not arm any partition until all battery trouble conditions are rectified.

6.3 NO ARMING ON TAMPER

SECTION [501]: OPTION [8]

With option [8] on in section [501], the control panel can restrict arming if the control panel detects a tamper on a zone or module (see section 7.4). The control panel will not arm any partition until all tamper trouble conditions are rectified and the Installer Code has been entered to clear the troubles.

6.4 NO ARMING ON SUPERVISION LOSS

SECTION [501]: OPTION [4]

With option [4] on in section [501], the control panel can restrict arming if the control panel receives a supervision loss signal from a wireless module (see section 7.3). The control panel will not arm

any partition until all supervision loss trouble conditions are rectified.

6.5 TIMED AUTO-ARMING

SECTIONS [505], [509], [513], [517]: OPTION [5]

With this option enabled, the control panel will arm the selected partition every day at the time specified by the Auto-Arm Timer (see section 6.5.1). When the partition is automatically armed, the control panel will transmit the *Auto-Arming* report code programmed in section [626]. Any open zones detected when a partition is Auto-Armed will be bypassed regardless of their definition (except 24hr. zones). The type of arming is determined by the *Auto-Arming Option* (see section 6.7). Regardless whether the partition was successfully armed or not, the control panel will always transmit the *Late to Close* report code programmed in section [626]. Please note that the control panel will enter a 60-second Exit Delay period before arming the system. At this point, Auto-Arming can be cancelled by entering a valid access code. Since the control panel can enable this feature for each individual partition, select the section that corresponds to the desired partition and turn on option [5].

[505] = Partition 1 [513] = Partition 3
[509] = Partition 2 [517] = Partition 4

6.5.1 Auto-Arm Timer

SECTIONS [271] TO [274]

If Timed Auto-Arming is enabled (see section 6.5), the control panel will send the *Late to Close* report code and attempt to arm the system at the time specified by the Auto-Arm Timer.

Sections [271] to [274] represent timers for partitions 1 through 4 respectively. Select the section corresponding to the partition and program the time you wish the control panel to arm the selected partition and/or send the *Late to Close* report code. Please note that the control panel will enter a 60-second Exit Delay period before arming the system. At this point, Auto-Arming can be cancelled by entering a valid access code.

Example:

A user would like to automatically arm partition 2 everyday at 6:15PM. To do so, enable "Timed Auto-Arming" for partition 2 by turning on option [5] in section [509]. Then enter 18:15 in section [272].

6.6 NO MOVEMENT AUTO-ARMING

SECTIONS [505], [509], [513], [517]: OPTION [6]

If no movement occurs in a partition's protected area for the period specified by the No Movement Timer (see section 6.6.1), the control panel will automatically arm that partition. The control panel will transmit the *No Movement* report code programmed in section [626] upon arming. The type of arming is determined by the Auto-Arming Option (see section 6.7). Regardless whether the partition was successfully armed or not, the control panel will always transmit the *Late to Close* report code (see section 8.2.2).

As the control panel can enable this feature for each individual partition, select the section that corresponds to the desired partition and turn on option [6].

[505] = Partition 1 [513] = Partition 3
[509] = Partition 2 [517] = Partition 4

6.6.1 No Movement Timer

SECTIONS [222] TO [225]

(001 to 255 X 15min.) If *No Movement Auto-Arming* is enabled (see section 6.6), the control panel can send the *No Movement* report code and attempt to arm the system if no movement has occurred for the period specified by the *No Movement Timer*.

If No Movement Auto-Arming is disabled, the control panel can still send the *No Movement* report code.

Sections [222] to [225] represent timers for partitions 1 through 4 respectively. Select the section corresponding to the desired partition and program the time (001 to 255 x15 minutes, 000 = disabled) without movement you wish the control panel to wait before arming and/or sending the *No Movement* report code.

Example:

A user would like to arm partition 1 whenever there is no movement for a period of 4 hours. First, enable the Auto-Arm on No Movement feature for partition 1 by turning on option [6] in section [505]. Then in section [222] enter 016 (16x15min. = 240min. = 4 hours).

6.7 AUTO-ARMING OPTIONS

SECTION [505], [509], [513], [517]: OPTION [7]

When using the Auto-Arming Features (see section 6.5 and section 6.6), the control panel can Force Arm or Stay Arm the selected partition. In the section corresponding to the desired partition set option [7]:

Option [7] ON = Stay Arming (see section 16.1.2)

Option [7] OFF = Force Arming (see section 16.1.6)

6.8 ONE-TOUCH FEATURES

[508], [512], [516], [520]: OPTIONS [1] TO [7]

The One-touch Features allow users to arm or disarm a partition without entering access codes. If the keypad is assigned to more than one partition, the feature must be enabled in the corresponding partitions. Select the section that corresponds to the desired partition and turn the desired options on or off:

REGULAR ARM

Option [1] ON

Press and hold the [ARM] key for 2 seconds to Regular Arm (see section 16.1.1)

STAY ARM

Option [2] ON

Press and hold the [STAY] key for 2 seconds to Stay Arm (see section 16.1.2)

INSTANT ARM

Option [3] ON

Press and hold the [5] key for 2 seconds to Instant Arm (see section 16.1.4)

FORCE ARM

Option [4] ON

Press and hold the [FORCE] key for 2 seconds to Force Arm (see section 16.1.6)

DISARM

Option [5] ON

Press and hold the [DISARM] key for 2 seconds to Disarm a Stay or Instant armed partition (see section 16.1.7)

BYPASS PROGRAMMING

Option [6] ON

Press and hold the [BYP] key for 2 seconds to perform Bypass Programming (see section 16.2).

EVENT RECORD DISPLAY

Option [7] ON

Press and hold the [7] key for 2 seconds to access the Event Record Display (see section 16.8).

6.9 EXIT DELAY

SECTIONS [226] TO [229]: 001-255 SECONDS

The Exit Delay determines the amount of time a user has to leave the protected area before the control panel arms the partition. Program the Exit Delay from 001 to 255 seconds, where sections [226] to [229] represent partitions 1 through 4 respectively. The Exit Delay applies to all zones in the selected partition except 24Hr. Zones.

6.9.1 Exit Delay Termination

SECTIONS [505], [509], [513], [517]: OPTION [8]

The control panel can reduce the Exit Delay to 5 seconds when an Entry Delay zone (see section 4.2.2) is opened and closed during the Exit Delay. Since the control panel can enable this feature for each individual partition, select the section that corresponds to the desired partition and turn on option [8].

Example:

A user arms a partition with an Exit Delay of 45 seconds. After 15 seconds, the user leaves the protected area through the front door (Entry Delay zone). When the door closes, the control panel reduces the remaining Exit Delay from 30 seconds to 5 seconds.

6.9.2 No Exit Delay on Remote Arm

SECTIONS [508], [512], [516], [520]: OPTION [8]

When a user arms by using a remote control from a wireless module (DGP-319 or OMN-RCV3), the control panel will cancel the Exit Delay and immediately arm the system.

6.10 KEYPAD LOCK-OUT FEATURE

SECTIONS [220] AND [221]

If a consecutive number of invalid codes are entered into the keypad, the control panel can be set to lockout access from that keypad for a specified period. Program the number of consecutive invalid codes from 001 to 255 (000 = disabled) into section [220]. Program the duration of the keypad lockout from 001 to 255 minutes into section [221]. Although programming 000 into section [221] will not lockout the keypad, the control panel will transmit the *Keypad Lockout* report code programmed in section [705].

6.11 MAXIMUM BYPASS ENTRIES

SECTIONS [238] TO [241]

Sections [238] to [241] represent Maximum Bypass Entries for partitions 1 through 4 respectively. Select the section corresponding to the desired partition and enter any value between 001 and 255 (000 = no limit) to determine the maximum number of zones that can be bypassed in a selected partition.

Example:

Section [238] is programmed with 010. When in Bypass Programming (see section 16.2), the control panel will not let the user bypass more than 10 zones in partition 1.

6.12 DISPLAY “BYPASS” IF ARMED

SECTION [504]: OPTION [5]

When option [5] is enabled, the keypad will not display that there are bypassed zones when the system is armed.

6.13 BELL SQUAWK

SECTIONS [507], [511], [515], & [519]: OPTIONS [1] TO [6]

Sections [507], [511], [515], and [519] represent partitions 1 through 4 respectively. Since the control panel can enable the Bell Squawk features for each individual partition, select the section that corresponds to the desired partition and turn on the desired option (when the option is off, the feature is disabled):

BELL SQUAWK UPON DISARMING

Option [1] ON

The bell or siren will emit two squawks upon disarming.

BELL SQUAWK UPON ARMING

Option [2] ON

The bell or siren will squawk once upon arming.

BELL SQUAWK ON AUTO-ARM

Option [3] ON

The bell or siren will squawk at 1-second intervals during the 60 seconds before a partition automatically arms itself. During the final 10 seconds of the 60-second period, the bell or siren will emit three squawks at 1-second intervals.

BELL SQUAWK DURING EXIT DELAY

Option [4] ON

The bell or siren will squawk at 1-second intervals during the Exit Delay. During the final 10 seconds of the Exit Delay, the bell or siren will emit three squawks at 1-second intervals.

BELL SQUAWK ON ENTRY DELAY

Option [5] ON

The bell or siren will squawk at 1-second intervals during the Entry Delay.

BELL SQUAWK ON REMOTE ARMING

Option [6] ON

When using a wireless module (DGP-319 or OMN-RCV3), the bell or siren will squawk once upon arming or disarming with a remote control.

6.14 RING-BACK

SECTIONS [507], [511], [515], [519]: OPTIONS [7] AND [8]

After disarming the system, the control panel can warn the user that there was an alarm and that it may be dangerous to enter by having the keypad beep 10 times and/or by squawking the bell 10 times. The user should leave immediately and contact the central station from a secure location. Sections [507], [511], [515], and [519] represent partitions 1 through 4 respectively. Since the control panel can enable the *Ring-Back* features for each individual partition, select the section that corresponds to the desired partition and turn on the desired option:

Option [7] ON = Bell Squawk Ring-Back Enabled

Option [8] ON = Keypad Ring-Back Enabled

6.15 SWITCH TO STAY ARMING

If no Entry Delay zones are opened and closed during the Exit Delay after Regular Arming a partition, the control panel can switch from Regular Arming to Stay Arming (see section 16.1). Since the control panel can enable *Switch to Stay Arming* for each individual partition, select the section that corresponds to the desired partition and turn on the corresponding option as listed below.

Section [505] = Partition 1 = Option [1]

Section [509] = Partition 2 = Option [2]

Section [513] = Partition 3 = Option [3]

Section [517] = Partition 4 = Option [4]

ALARM OPTIONS

7.1 BELL/ALARM OUTPUT

SECTION [500]: OPTIONS [5] TO [8]

When a partition generates an alarm, the control panel can toggle the on-board BELL/ALARM output enabling any bells or sirens connected to it. Since the control panel can enable this feature for each individual partition, in section [500] turn on the option that corresponds to the desired partition, where options [5] to [8] represent partitions 1 through 4 respectively.

7.2 BELL CUT-OFF TIMER

SECTIONS [234] TO [237]

After an audible alarm, the bell or siren will stop once the partition is disarmed or when the Bell Cut-Off Timer has elapsed. Sections [234] to [237] represent partitions 1 through 4 respectively. Since the control panel can set a Bell Cut-Off Timer for each individual partition, select the section corresponding to the desired partition and enter any value between 001 and 255 minutes (000 = 4 minutes).

7.2.1 No Bell Cut-Off on Fire Alarm

SECTION [502]: OPTION [8]

The control panel can disable the Bell Cut-Off Timer when alarms are generated from zones defined as Standard or Delayed Fire Zones (see section 4.2). The bell/siren output will remain enabled until a user disarms the partition in alarm.

7.2.2 Recycle Alarm Rate

SECTIONS [246] TO [249]

Once an alarm has occurred, the control panel will re-verify the zone status at a programmed rate once the Bell Cut-Off Timer and the Recycle Delay have elapsed. If any open zones remain, the control panel will regenerate the alarm. The number of times in one armed period that the control panel will re-verify the zone status after the Bell Cut-off occurs is programmed in sections [246] to [249], which represent partitions 1 through 4. Enter rate from 001 to 255 (000 = no limit).

7.2.3 Recycle Delay

SECTIONS [242] TO [245]

The Recycle Delay is the amount of time the control panel will wait after the Bell Cut-off occurs before re-verifying the zone status. In the section corresponding to the desired partition, program the Recycle Delay from 001 to 255 minutes (000 = disabled). Sections [242] to [245] represent partitions 1 through 4.

7.3 WIRELESS TRANSMITTER SUPERVISION OPTIONS

SECTION [501]: OPTIONS [1] AND [2]

The Supervision feature must be enabled in a wireless module (DGP-319 or OMN-RCV3) in order for this feature to function. When the control panel receives a Supervision Loss message (wireless receiver no longer receiving signals from a wireless transmitter) in an armed partition, the control panel will generate an alarm unless the Wireless Transmitter Supervision Options have been disabled. Alarms will be silent or audible depending on individual zone settings.

If a supervision loss occurs in a disarmed partition, the control panel will follow the programmed settings:

DISABLED

[1] OFF and [2] OFF

When a supervision loss occurs, the control panel will display the zone as open in the keypad display, but will not generate an alarm or a trouble. *This option is not permitted on UL systems.*

TROUBLE ONLY

[1] OFF and [2] ON

If a partition is armed, the control panel will generate a standard alarm when a supervision loss occurs. If the partition is disarmed when a supervision loss occurs, the *Zone Fault* trouble will appear in the keypad's Trouble Display and the control panel will transmit the appropriate report code (see section 8.2).

SILENT ALARM

[1] ON and [2] OFF

If a partition is armed, the control panel will generate a standard alarm when a supervision loss occurs. If the partition is disarmed when a supervision loss occurs, the *Zone Fault* trouble will appear in the keypad's Trouble Display, the control panel will transmit the appropriate report code (see section 8.2), and it will also generate a silent alarm (no bells or sirens).

AUDIBLE ALARM

[1] ON and [2] ON

If a partition is armed, the control panel will generate a standard alarm when a supervision loss occurs. If the partition is disarmed when a supervision loss occurs, the *Zone Fault* trouble will appear in the keypad's Trouble Display, the control panel will transmit the appropriate report code (see section 8.2), and it will also generate an audible alarm.

7.3.1 Supervision Bypass Options

SECTION [501]: OPTION [3]

With option [3] enabled in section [501], the Wireless Transmitter Supervision Options will follow the zone's bypass definition. This means that the control panel will not perform any action if a supervision loss occurs on a bypassed zone. With option [3] disabled, the control panel will ignore the bypass definition and will follow the option set in section 7.3 if a supervision loss occurs on a bypassed zone.

7.4 TAMPER RECOGNITION OPTIONS

SECTION [501]: OPTIONS [5] AND [6]

Regardless of the Tamper Recognition Options, if a tamper or wire fault occurs on a zone or on an expansion module in an armed partition, the control panel will **always** generate an alarm unless Tamper Recognition has been disabled. Alarms will be silent or audible depending on individual zone settings.

If a tamper or wire fault occurs on a zone or on an expansion module in a **disarmed** partition, the control panel will follow the programmed settings:

TAMPER RECOGNITION DISABLED

[5] OFF and [6] OFF

If a **partition is armed**, the control panel will generate a standard alarm when a tamper or wire fault occurs. **If the partition is disarmed**, the control panel will display the zone as open in the keypad display, but will not generate an alarm or a trouble. *This option is not permitted on UL systems.*

TROUBLE ONLY

[5] ON and [6] OFF

If a **partition is armed**, the control panel will generate a standard alarm when a tamper or wire fault occurs. **If the partition is disarmed** when a tamper or wiring failure occurs, the appropriate trouble will appear in the keypad's Trouble Display and the control panel will transmit the appropriate report code (see section 8.2).

SILENT ALARM

[5] OFF and [6] ON

If a **partition is armed**, the control panel will generate a standard alarm when a tamper or wire fault occurs. **If the partition is disarmed** when a tamper or wiring failure occurs, the appropriate trouble will appear in the keypad's Trouble Display, the control panel will transmit the appropriate report code (see section 8.2), and it will generate a silent alarm (no bells or sirens).

AUDIBLE ALARM

[5] ON and [6] ON

If a **partition is armed**, the control panel will generate a standard alarm when a tamper or wire fault occurs. **If the partition is disarmed** when a tamper or wiring failure occurs, the appropriate trouble will appear in the keypad's Trouble Display, the control panel will transmit the appropriate report code (see section 8.2), and it will generate an audible alarm.

7.4.1 Tamper Bypass Options

SECTION [501]: OPTION [7]

With option [7] enabled in section [501], Tamper Recognition follows the zone bypass definition. This means that the control panel will not perform any action if a tamper or wire fault occurs on a bypassed zone. With option [7] disabled, the control panel will ignore the zone's bypass definition and will follow the option set in section 7.4 if a tamper or wire fault occurs on a bypassed zone.

7.5 KEYPAD PANIC OPTIONS

SECTIONS [506], [510], [514], [518]: OPTIONS [1] TO [6]

Since the control panel can enable Keypad Panic Options for each individual partition, select the section that corresponds to the desired partition and set options [1] through [6] on/off to obtain the desired options. Sections [506], [510], [514], and [518] represent partitions 1 to 4 respectively.

PANIC 1

Option [1] ON

Press the [1] and [3] keys simultaneously on the keypad for 2 seconds to generate a silent or audible alarm defined by option [4].

Option [4] ON = Panic 1 is Silent

Option [4] OFF = Panic 1 is Audible

PANIC 2

Option [2] ON

Press the [4] and [6] keys simultaneously on the keypad for 2 seconds to generate a silent or audible alarm defined by option [5].

Option [5] ON = Panic 2 is Silent

Option [5] OFF = Panic 2 is Audible

PANIC 3

Option [3] ON

Press the [7] and [9] keys simultaneously on the keypad for 2 seconds to generate a silent or pulsed alarm defined by option [6].

Option [6] ON = Panic 3 is Silent

Option [6] OFF = Panic 3 is Pulsed (Fire)

SILENT OPERATION

The control panel emits a single Confirmation Beep and transmits the appropriate report code (see section 8.2.5) to the central station.

AUDIBLE OPERATION

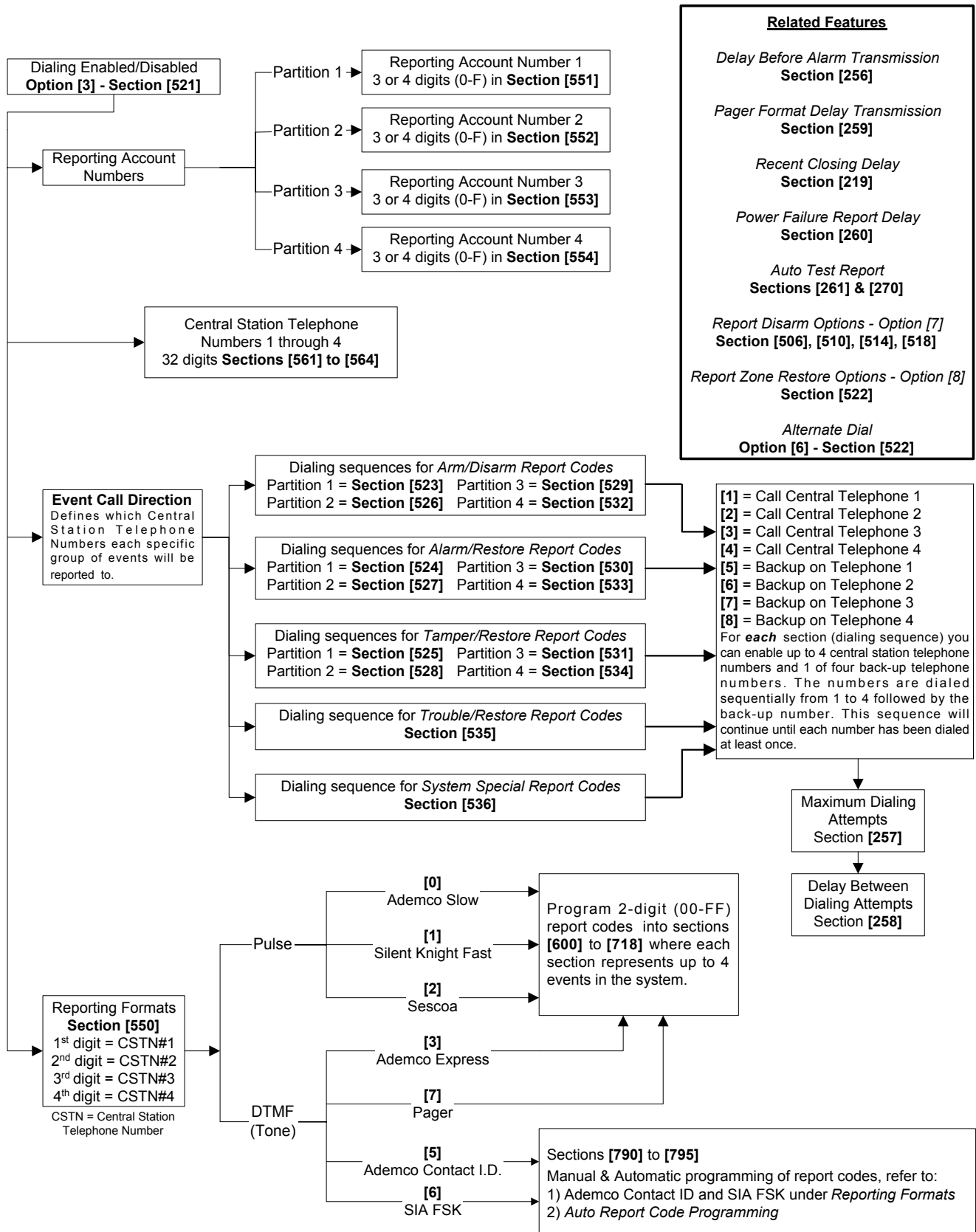
The alarm output (bell/siren) activates until a user cancels the alarm with a valid User Access Code or when the Bell Cut-Off Timer elapses (see section 7.2).

FIRE OPERATION

Same as audible operation, except that the bell/siren output will be pulsed as shown in Figure 4-4 on page 16.

EVENT REPORTING

Figure 8-1: Event Reporting



8.1 REPORTING ENABLED

SECTION [521]: OPTION [3]

This option will either enable or disable event reporting. With option [3] on in section [521], Event Reporting will be enabled. When an event (e.g. open zone) occurs in the system, the control panel verifies if a report code was programmed in the section corresponding to the event. If a report code is programmed, the control panel will dial the central station telephone number defined by the Event Call Direction feature. When the central station answers, the control panel will transmit the system account code, followed by the programmed report code.

8.2 REPORT CODES

A report code is a 2-digit or 1-digit hexadecimal value, consisting of digits from 0 to F. Each section from [600] to [718] represents a set of four specific events. Each of these events can be programmed with a 1-digit or 2-digit report code. For a comprehensive list of the events and their relevant sections, please refer to the *Digiplex Programming Guide*. Please note that only the Ademco Slow, Silent Knight, Sescoa and Pager Formats support 1-digit report codes.

When a specific event occurs, the control panel will send the programmed report code to the central station. The method of report code transmission is defined by the following two items: **Reporting Formats** (see section 8.5) and **Event Call Direction** (see section 8.6). These two items define how and where the report codes are transmitted. If you are using the Ademco CID or SIA formats, an Auto Report Code Programming feature is available. Using this feature, sections [600] to [718] do not have to be manually programmed (see section 8.13). The following sub-sections provide a brief description of the events that the control panel can report:

8.2.1 Arming Report Codes

SECTIONS [600] TO [625]

A report code can be programmed for each of the 96 User Access Codes and 8 keyswitch zones. When using an access code or keyswitch to arm one or more partitions, the control panel can send the appropriate report code to the central station identifying which access code or keyswitch zone was used to arm the partition(s).

8.2.2 Special Arming Report Codes

SECTIONS [626] TO [627]

Whenever the system is armed using one of the special arming features, the control panel can send the appropriate report code to the central station identifying how the system was armed.

Section [626]

- Auto-Arming (see section 6.5)
- PC Arming: system armed using WinLoad (see section 15)
- Late to Close (see section 6.5)
- No Movement (see section 6.6)

Section [627]

- Partial Arming: when partitions are Stay Armed, Instant Armed or armed with bypassed zones
- Quick Arming: partitions armed using any of the One-Touch Arming features (see section 6.8)

8.2.3 Disarming Report Codes

SECTIONS [628] TO [653]

A report code can be programmed for each of the 96 User Access Codes and 8 keyswitch zones. Whenever an access code or keyswitch is used to disarm one or more partitions, the control panel can send the appropriate report code to the central station identifying which access code or keyswitch was used to disarm the partition(s). The control panel can transmit the report codes every time a partition is disarmed or only when disarmed following an alarm. Please refer to Disarm Reporting Options in section 8.10.

8.2.4 Special Disarming Report Codes

SECTION [654]

Whenever using one of the special disarming features listed below, the control panel can send the report code to the central station identifying how the system was disarmed. The control panel can transmit the report codes every time a partition is disarmed or only when disarmed following an alarm. Please refer to Disarm Reporting Options in section 8.10.

Section [654]

- Cancel Auto-Arm: if a user disarms the partition during the Auto-Arm 60-second delay
- Quick Disarm: partitions disarmed using the One-Touch Disarming feature (see section 6.8)
- PC Disarm: when WinLoad is used to disarm the system

8.2.5 Zone Alarm Report Codes

SECTIONS [655] TO [666]

A report code can be programmed for each of the 48 available zones. Whenever a zone generates an alarm, the control panel can send the appropriate report code to the central station identifying which zone generated an alarm.

8.2.6 Zone Restore Report Codes

SECTIONS [667] TO [678]

A report code can be programmed for each of the 48 available zones. The control panel can transmit these report codes to the central station when the zone closes after generating an alarm or once the bell has cut-off after alarm generation (see section 7.2). Please refer to Zone Restore Report Options in section 8.11.

8.2.7 Special Alarm Report Codes

SECTIONS [679] TO [680]

Whenever the system generates an alarm due to one of the conditions listed below, the control panel can send the appropriate report code to the central station identifying the type of alarm.

Section [679]

- Emergency Panic: if the panic keys [1] and [3] have been pressed (see section 7.5)
- Auxiliary Panic: if the panic keys [4] and [6] have been pressed (see section 7.5)
- Fire Panic: if the panic keys [7] and [9] have been pressed (see section 7.5)
- Recent Closing: if after having armed the system, an alarm is generated within the *Recent Close Delay* (see section 8.7)

Section [680]

- Auto Zone Shutdown: a zone communicates more than the programmed number of transmissions in a single armed period (see section 4.4.1)
- Duress: a Duress enabled access code is keyed in (see section 13.5.2).

8.2.8 Zone Tamper Report Codes

SECTION [681] TO [692]

A report code can be programmed for each of the 48 available zones. Whenever a tamper or wire fault occurs on a zone, the control panel can send the appropriate report code to the central station identifying which zone was tampered. If the Tamper Recognition Options (see section 7.4) are disabled, the control panel will not report the occurrence of any tampers or wire faults.

8.2.9 Zone Tamper Restore Codes

SECTIONS [693] TO [704]

A report code can be programmed for each of the 48 available zones. Whenever a tampered zone is restored, the control panel can send the appropriate report code to the central station identifying which zone has been restored.

8.2.10 Special Tamper Report Codes

SECTION [705]

- Keypad Lockout: (see section 6.10)

8.2.11 System Trouble Codes

SECTIONS [706] TO [711]

Section [706]

- AC Failure: no AC input detected on the control panel. The control panel can delay reporting this event, please refer to Power Fail Report Delay in section 8.9.
- Battery Failure: the back up battery is disconnected or the battery voltage is less than or equal to 10.5V
- Auxiliary Supply: the auxiliary power supply's current is greater than or equal to 1.1A.

Section [707]

- Bell Output: the bell/siren output is disconnected or the current is greater than or equal to 3A
- Clock Loss: the control panel detects a loss in panel time (see section 12.7)
- Fire Loop Trouble: a tamper has been detected on a fire zone (see section 4.2)
- N/A

Section [708]

- Network Fault: a module has been removed from the network.
- Module Tamper: a tamper or wire fault is detected on a module other than a motion detector connected to the network
- ROM Check Error: problem with on-board Read-Only Memory
- Module TLM: TLM failure detected on voice dialer connected to the network

Section [709]

- Module Fail to Communicate: a voice dialer has failed to communicate with the central station
- Printer Fault: the Printer Module connected to the network has detected an error (see the Printer Module Manual for details).
- Module AC Failure: no AC power detected on a module connected to the communication network
- Module Battery Failure: the backup battery on a module is disconnected or the battery voltage is low

Section [710]

- Module Auxiliary Failure: the auxiliary output of a module connected to the network has exceeded current limits
- Wireless Transmitter Low Battery
- Wireless Module Supervision Failure: This report code is global unless using the Contact ID or SIA reporting formats.

Section [711]

- Phone Number 1 Fail to Communicate
- Phone Number 2 Fail to Communicate
- Phone Number 3 Fail to Communicate
- Phone Number 4 Fail to Communicate

Please note: there is no Fail to Communicate for Pager telephone numbers.

8.2.12 System Trouble Restore Codes

SECTION [712] TO [716]

Section [712]

- TLM: a TLM failure has restored.



If the Telephone Line Monitoring (see section 9.1) is disabled, the control panel will not transmit the TLM report code.

- AC Failure Restored
- Battery Failure Restored
- Auxiliary Supply Restored

Section [713]

- Bell Output Restored
- Time programmed
- Fire Loop Trouble Restored
- N/A

Section [714]

- Network Fault Restored
- Module Tamper Restored
- ROM Check Error Restored
- Module TLM Restored

Section [715]

- Printer Fault Restored
- Module AC Failure Restored
- Module Battery Failure Restored

Section [716]

- Module Auxiliary Failure Restored
- Wireless Transmitter Low Battery Restored
- Wireless Module Supervision Restored: This report code is global unless using the Contact ID or SIA Reporting formats.

8.2.13 Special Reporting Codes

SECTION [717] AND [718]

Whenever the system generates one of the following instances, the control panel can send the appropriate report code to the central station identifying the type of system occurrence:

Section [717]

- Cold Start: the control panel was completely shutdown (total power loss) and the control panel was re-started
- Warm Start: the control panel performs a reset due to any sudden problem other than power loss
- Test Report: report generated automatically (see section 8.8)

Section [718]

- WinLoad Access: the panel ended communication with WinLoad
- Installer In: installer has entered the programming mode
- Installer Out: installer has exited the programming mode

8.3 CENTRAL STATION PHONE

SECTIONS [561] TO [564]

The Digiplex Control Panel can dial up to 4 different central station telephone numbers. Sections [561] to [564] represent central station telephone numbers 1 through 4. You can enter any digit from 0 to 9 and any special keys or functions (see Table 3, *Special Telephone Number Keys*) up to a maximum of 32 digits. Refer to Event Call Direction in section 8.6 and Reporting Formats in section 8.5 for details on how these telephone numbers are used.



For North American installations using either SIA or Contact ID reporting formats (see section 8.5), enter *70 before the phone number to disable call-waiting.

Table 3: Special Telephone Number Keys

[STAY]	= *
[FORCE]	= #
[ARM]	= Switch to Tone Dialing (T)
[DISARM]	= Wait for second dial tone (W)
[BYP]	= 4-second pause (P)
[MEM]	= Insert
[TRBL]	= Delete
[ACC]	= Delete from cursor to the end

8.4 PARTITION ACCOUNT

SECTIONS [551] TO [554]

All report codes are preceded by a 4-digit or 3-digit Partition Account Number to ensure correct identification of active zones in a partitioned system. Sections [551] to [554] represent the Partition Account Codes for partitions 1 through 4. Partition account numbers can be any hexa-digit from 0 to F.

Example:

If a zone generates an alarm in Partition 1, the control panel will send Partition Account Number 1 followed by the report code.



Only the SIA format supports the [0] = 0 digit in its account numbers. Account numbers that use any other reporting format do not support the [0] = 0 digit. You must enter the [STAY] = A digit in its place. When using the SIA Format, the control panel will only use Partition Account Number 1 programmed in section [551], but the report code will include the partition number.

8.5 REPORTING FORMATS

SECTION [550]

The Digiplex Control Panel can use a number of different reporting formats and each of the four Central Station Phone Numbers (see section 8.3) should be programmed with the same reporting format unless it is combined with a Pager format. The first digit entered into section [550] represents the reporting format (see Table 4, *Reporting Formats*) used to communicate with central station telephone number 1, the second digit represents telephone number 2 and so forth.

Table 4: Reporting Formats

0 = Ademco slow (1400Hz, 1900Hz, 10BPS)
1 = Silent Knight fast (1400Hz, 1900Hz, 20BPS)
2 = SESCOA (2300Hz, 1800Hz, 20BPS)
3 = Ademco Express (DTMF 4+2)
4 = Reserved for future use
5 = Ademco Contact ID
6 = SIA FSK
7 = Pager

8.5.1 Standard Pulse Formats

The Digiplex Control Panel can use the Ademco slow, Silent Knight fast and SESCOA standard pulse reporting formats (see Table 4, *Reporting Formats*).

8.5.2 Ademco Express

The Ademco Express is a high-speed reporting format that communicates 2-digit (00 to FF) report codes programmed into sections [600] to [718]. Unlike other Ademco formats, the Ademco Express does not use the Contact ID Report Codes.

8.5.3 Ademco Contact ID

Ademco Contact ID is a fast communicator format that uses tone reporting instead of pulse reporting. This communicator format also uses a pre-defined list of industry standard messages and report codes that will suit most of your basic installation needs. To manually program the report codes, key in the 2-digit hexadecimal values from the *Contact ID Report Codes List* in the *Programming Guide* into the desired report codes in sections [600] to [718] (see section 8.2). You can also enter 00 to disable reporting or FF to use the default report code from the *Automatic Report Code List* in the *Programming Guide*. To automatically program a set of default Contact ID codes, refer to section 8.13.

8.5.4 SIA FSK

SIA FSK is a fast communicator format that uses tone reporting instead of pulse reporting. This communicator format uses a pre-defined list of industry standard messages and report codes that will suit most of your basic installation needs. To manually program the report codes, enter 00 to disable reporting or FF to use the

default report code from the *Automatic Report Code List* in the *Programming Guide*. To automatically program a set of default SIA FSK codes, refer to section 8.13.

8.5.5 Pager Reporting Format

Using this format allows the control panel to transmit report codes to a pager. A pound symbol “#” is automatically generated after the report code. Please refer to Pager Delay in section 8.12.

8.6 EVENT CALL DIRECTION

SECTIONS [522] TO [536]

As shown in Figure 8-1 on page 25, the control panel events are divided into three event groups for each partition and two global event groups. Each event group can be programmed to dial up to four central station telephone numbers and to use one of the four telephone numbers as a backup. The numbers are dialed sequentially starting from 1, skipping any disabled numbers and stopping once all selected telephone numbers have been reached. If the control panel still fails to report to a central station telephone number after reaching the Maximum Dialing Attempts (see section 8.6.1), the control panel will dial the selected backup telephone number unless the Alternate Backup Option is enabled (see section 8.6.3). When the Alternate Backup Option is enabled, the control panel will dial the backup number after every failed attempt.

8.6.1 Maximum Dialing Attempts

SECTION [257]

The number (001 to 255) programmed into section [257] determines how many times the control panel will dial the same central station telephone number before proceeding to the next number. Also refer to section 8.6.3.

8.6.2 Delay Between Dialing Attempts

SECTION [258]

This delay will determine the amount of time the control panel will wait between dialing attempts. This delay can be set from 001 to 255 seconds.

8.6.3 Alternate Backup Option

SECTION [522]: OPTION [6]

With option [6] enabled in section [522], the control panel will dial the selected backup telephone number after every failed attempt to contact a central station telephone number. Otherwise (option [6] off), the control panel will only dial the backup telephone number after the Maximum Dialing Attempts (see section 8.6.1) to one central station telephone number have failed.

8.7 RECENT CLOSE DELAY

SECTION [219]

If after having armed the system, an alarm is generated within the period programmed into section [219] (000 to 255 seconds), the control panel will transmit the *Recent Close* report code programmed into section [679].

8.8 AUTO TEST REPORT

SECTIONS [261] AND [270]

The control panel will transmit the test report code programmed into section [717] after the number of days (000 to 255)

programmed into section [261] has elapsed and at the time (00:00 to 23:59) programmed into section [270].

8.8.1 Hourly Test Transmission

SECTION [522]: OPTION [3]

Alternatively, the control panel can transmit the test report code programmed into section [717] every hour. Turn off option [3] to disable this feature. Program the minute of each hour (00:00 to 00:59) it sends the test report into section [270].

8.9 POWER FAIL REPORT DELAY

SECTION [260]

The control panel will delay transmission of the *AC Failure* report code programmed into section [712] by the period programmed into section [260] (000 to 255 minutes).

8.10 DISARM REPORTING OPTIONS

SECTIONS [506], [510], [514], [518]: OPTION [7]

Since the control panel can enable the Disarm Reporting Options for each individual partition, select the section that corresponds to the desired partition and turn option [7] on or off as desired. Sections [506], [510], [514], [518] represent partitions 1 to 4 respectively.

REPORT ON DISARM AFTER ALARM ONLY

Option [7] ON

The Digiplex Control Panel will send Disarming Report Codes (see section 8.2.3) to the central station only when the system is disarmed following an alarm.

REPORT ON DISARM

Option [7] OFF

The Digiplex Control Panel will send the Disarming Report Codes (see section 8.2.3) to the central station whenever a partition is disarmed.

8.11 ZONE RESTORE REPORT OPTIONS

SECTION [522]: OPTION [8]

REPORT ON ZONE CLOSURE

Option [8] ON

The control panel will send the *Zone Alarm Restore* report codes (see section 8.2.6) to the central station as soon as the zone returns to normal (zone closure) or upon disarming

REPORT ON BELL CUT-OFF

Option [8] OFF

The control panel will send the *Zone Alarm Restore* report codes (see section 8.2.6) to the central station when the Bell Cut-Off Timer has elapsed or when the alarm has been disarmed (see section 7.2).

8.12 PAGER DELAY

SECTION [259]

When using the Pager Reporting Format (see section 8.5.5), the control panel will wait for the delay period programmed into section [259] (001 to 060 seconds) before uploading the report codes to

the pager. This is to allow time for the pager system to provide a dial tone or to bypass the welcome message before sending data.

8.13 AUTO REPORT CODE PROGRAMMING

SECTIONS [790] TO [795]

When using either the Contact ID or SIA Reporting Formats (see section 8.5), the Digiplex system can automatically program a set of default report codes. From programming mode (see section 3.1) enter any of the following sections to set the indicated report codes:

ALL CODES

Section [790]

Sets all report codes in sections [600] to [718] with the default values from the *Automatic Report Codes List* in the *Programming Guide*.

ARMING & DISARMING CODES

Section [791]

Sets all report codes in sections [600] to [654] with the default values from the *Automatic Report Codes List* in the *Programming Guide*.

ALARM RESTORE CODES

Section [792]

Sets all report codes in sections [655] to [680] with the default values from the *Automatic Report Codes List* in the *Programming Guide*.

TAMPER & TAMPER RESTORE CODES

Section [793]

Sets all report codes in sections [681] to [705] with the default values from the *Automatic Report Codes List* in the *Programming Guide*.

TROUBLE RESTORE CODES

Section [794]

Sets all report codes in sections [706] to [716] with the default values from the *Automatic Report Codes List* in the *Programming Guide*.

SPECIAL CODES

Section [795]

Sets all report codes in sections [717] to [718] with the default values from the *Automatic Report Codes List* in the *Programming Guide*.

Please note that even after automatic report codes have been set, you can still use the manual programming method (see section 8.5.3 & section 8.5.4) to program remaining report codes or change some of the defaults.

DIALER OPTIONS

9.1 TELEPHONE LINE MONITORING

SECTION [521]: OPTIONS [1] AND [2]

When enabled, the system verifies the existence of a telephone line once every second. After each successful test, the dialer LED (green light) on the control panel flashes briefly. A line test failure occurs when the TLM detects less than 3 volts for the period defined by the TLM Fail Timer (see section 9.1.1). If the line test fails, the dialer LED will flash and will generate one or more conditions as defined by the TLM settings below, until the control panel detects the telephone line again. Please note that when the dialer detects a telephone ring, the TLM test stops for 1 minute.

TLM DISABLED

[1] OFF and [2] OFF

TROUBLE ONLY

[1] ON and [2] OFF

Upon line test failure, the *Communicator* trouble will appear in the keypad's Trouble Display.

ALARM IF SYSTEM ARMED

[1] OFF and [2] ON

Upon line test failure, the *Communicator* trouble will appear in the keypad's Trouble Display and the control panel will generate an alarm if the system is armed.

SILENT ALARM BECOMES AUDIBLE

[1] ON and [2] ON

Upon line test failure, the *Communicator* trouble will appear in the keypad's Trouble Display and cause a *Silent Alarm* zone or *Silent* panic alarm to switch to an audible alarm.

9.1.1 TLM Fail Timer

SECTION [255]

If the TLM does not detect the existence of a telephone line for the time programmed in this section, the control panel will generate the condition(s) defined by the TLM options (see section 9.1). Enter any value between 016 and 255 (value is X2 seconds) into section [255]. Entering a value between 000 and 016 will set the TLM Fail Timer to 32 seconds.

9.2 TONE/PULSE DIALING

SECTION [521]: OPTION [4]

Option [4] ON = the control panel can dial using the tone/DTMF format.

Option [4] OFF = the control panel will use the pulse dialing format. Refer to section 9.3 for setting the pulse ratio.

9.3 PULSE RATIO

SECTION [521]: OPTION [5]

When using Pulse dialing (see section 9.2), you can select one of two Pulse Ratios. Although most European countries use the 1:2 pulse ratio, the 1:1.5 ratio may provide better results in some cases. The same applies for North American countries. If the 1:1.5

pulse ratio is not providing the desired results, the 1:2 ratio may be used.

Option [5] ON = North American pulse ratio of 1:1.5

Option [5] OFF = European pulse ratio of 1:2

9.4 BUSY TONE DETECTION

SECTION [521]: OPTION [6]

Option [6] ON = the control panel can immediately hang up if it receives a busy signal when dialing an outside number.

Option [6] OFF = feature disabled

9.5 SWITCH TO PULSE

SECTION [521]: OPTION [7]

Option [7] ON = When reporting events to the central station, the control panel can switch from tone dialing to pulse dialing on the fifth attempt. The control panel continues to use pulse dialing until it establishes communication. If switching to another central station telephone number, the control panel will return to tone dialing and will switch back to pulse dialing on the fifth attempt.

Option [7] OFF = Feature disabled

9.6 BELL ON COMMUNICATION FAIL

SECTION [521]: OPTION [8]

Option [8] ON = If the control panel fails to communicate with the central station when the system is armed, the control panel can enable the BELL output, which will set off any bells or sirens connected to the output.

Option [8] OFF = Feature disabled

9.7 DIAL TONE DELAY

SECTION [522]: OPTION [7]

Option [7] ON = Dialer will hang up if no dial tone is present after 32 seconds

Option [7] OFF = Dialer will continue to dial if no dial tone is present after 3 seconds. If more time is required, you can insert a 4-second pause into the desired telephone number sequence (see section 8.3).

PROGRAMMABLE OUTPUTS

A PGM is a programmable output that toggles to its opposite state (i.e. a normally open PGM will close) when a specific event has occurred in the system.

For example, a PGM can be used to reset smoke detectors, activate strobe lights, open/close garage doors and much more.

When a PGM closes, the control panel supplies a ground to the PGM activating any device or relay connected to it. When a PGM opens, the circuit opens from ground therefore not providing any power to devices connected to it. The control panel provides a maximum of 100mA to PGM1 and 50mA to PGMs 2, 3 and 4. PGM1 to PGM4 are normally open outputs and PGM5 is a normally open or normally closed 5A relay. For information on how to connect a relay to a PGM, please refer to section 2.9.

10.1 PGM ACTIVATION EVENT

SECTIONS [400], [402], [404], [406], AND [408]

The PGM Activation Event will activate the selected PGM when a specific event or events occur in the system. The control panel can set separate activation events for each PGM.

For example, the control panel can be programmed to activate PGM2 whenever the system is Force Armed.

To program a PGM activation event:

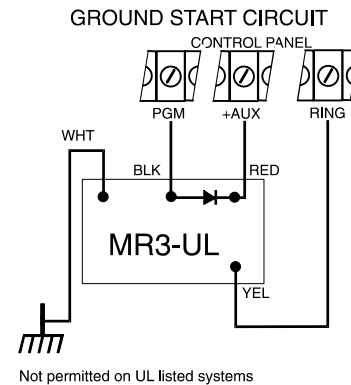
- 1) Enter the section that represents the desired PGM.
PGM1 = [400] PGM4 = [406]
PGM2 = [402] PGM5 = [408]
PGM3 = [404]
- 2) Enter the first digit (see *PGM Programming Table* on page 34) where each digit from 0 to F represents a specific group of events.
- 3) Enter the second digit, which can be any digit from 0 to F depending on the first digit.
- 4) After entering the second digit, use the Feature Select method (enable/disable options [1] to [8]) to select up to eight specific events as detailed in the *PGM Programming Table*.

For details on the available activation events please refer to the *PGM Programming Table* on page 34. Below you will find brief details on just a few of the available activation events:

Smoke Reset: Deactivates the PGM for a period of 4 seconds every time the [CLEAR] and [ENTER] keys are pressed simultaneously and held for 2 seconds. Please refer to section 2.15.3 for instructions on connecting the PGM in order to perform a smoke detector reset. Program First Digit = [4], Second Digit = [1], then [5] on.

Ground Start: Just before the control panel attempts to dial an outside line when using ground start telephone equipment, the PGM will activate for the period defined by the PGM Delay (see section 10.2.2). Please note that the PGM Deactivation Option must be set to Timed (see section 10.2). Program First Digit = [4], Second Digit = [1], then [6] on.

Figure 10-1: Ground Start Circuit



Kissoff: After receiving a handshake from the central station, the control panel activates the PGM for the period defined by the PGM Delay (see section 10.2.2). This can be used to latch the central station connection to another device such as a microphone/speaker module. Please note that the PGM Deactivation Option must be set to Timed (see section 10.2). Program First Digit = [4], Second Digit = [1], then [7] on.

Strobe: Activates the PGM whenever the system is in alarm. The PGM will remain activated even after Bell Cut-off and will wait until the alarm is cancelled before deactivating the PGM. Program First Digit = [1], Second Digit = choose [PARTITION] (0 = all enabled partitions, 8 = any enabled partition), then [5] on.

10.2 PGM DEACTIVATION OPTION

SECTION [502]: OPTIONS [1] TO [5]

Once the PGMs are activated (see section 10.1) they will deactivate according to the options programmed in section [502]. Options [1] to [5] represent PGMs 1 to 5 respectively. Each PGM can be set to Follow or Timed by turning the option representing the PGM on or off:

For example, if option [1] is on in section [502], then PGM1 is set to Timed.

FOLLOW

Option OFF

- 1) If the first digit of the PGM Activation Event is set at 1, 2, 3, 4, 5, 6, or 7, the PGM will remain activated until the PGM Activation Event has ended. It will ignore the PGM Deactivation Event.
- 2) If the first digit of the PGM Activation Event is set at 8, 9, A, B, C, D, E, or F, the PGM will remain activated until the PGM Deactivation Event occurs.

TIMED

Option ON

After activating the PGM, the control panel will start the PGM Delay Timer (see section 10.2.2) and the PGM will deactivate only when the PGM Delay Timer has elapsed and will ignore the PGM Deactivation Event.

10.2.1 PGM Deactivation Event

SECTIONS [401], [403], [405], [407], AND [409]

If the PGM Deactivation Option is set to Follow (see section 10.2), the PGM will deactivate when the programmed event occurs unless the first digit of the PGM Activation Event is 1 to 7. To program a PGM Deactivation Event:

- 1) Enter the section that represents the desired PGM.
PGM1 = [401] PGM4 = [407]
PGM2 = [403] PGM5 = [409]
PGM3 = [405]
- 2) Enter the first digit (see *PGM Programming Table* on page 34) where each digit from 0 to F represents a specific group of events.
- 3) Enter the second digit, which can be any digit from 0 to F depending on the first digit.
- 4) After entering the second digit, use the Feature Select method (enable/disable options [1] to [8]) to select up to eight specific events as detailed in the *PGM Programming Table*.

If the PGM Deactivation Option is set for Timed (see section 10.2), the PGM will ignore the PGM Deactivation Event.

10.2.2 PGM Delay Timers

SECTIONS [250] TO [254]

To program the PGM Delay Timers, enter the section that corresponds to the desired PGM, where sections [250] to [254] represent PGM1 to PGM5 respectively, and enter a value from 001 to 255. The value entered is either in seconds or minutes as determined by the PGM Time Base Selection (see section 10.2.3).

10.2.3 PGM Time Base Selection

SECTION [503]: OPTIONS [1] TO [5]

The PGM Time Base Selection determines whether the Delays programmed in sections [250] to [254] are in minutes or seconds. Options [1] to [5] represent PGMs 1 to 5 respectively. Each PGM Delay Timer can be set to minutes or seconds by turning the options on or off in section [503]:

Option ON = Minutes
Option OFF = Seconds

10.3 PGM1 Is SMOKE INPUT

SECTION [502]: OPTION [7]

Enabling option [7] in section [502] will set PGM1 to act as a zone input for two-wire smoke detectors. When programming Zone Numbering (see section 4.1), the control panel will recognize PGM1 as input number 255. For more information on how to connect two-wire smoke detectors, please refer to section 2.15.1

PGM PROGRAMMING TABLE

***Note1:** 0 = All partitions enabled in the system (see section 12.5)
 1 = Partition 1 3 = Partition 3
 2 = Partition 2 4 = Partition 4
 8 = Any partition enabled in the system (at least one)

First Digit	Event	Second Digit	Feature Select Programming							
			1	2	3	4	5	6	7	8
0	PGM Disabled	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
1	Status 1	Note 1*	Any Arming Method	Force Arm	Stay Arm	Instant Arm	Strobe (until alarm is cancelled)	Silent Alarm (until alarm is cancelled)	Audible Alarm (until alarm is cancelled)	Fire Alarm (until alarm is cancelled)
2	Status 2	Note 1*	Ready Status	Exit Delay	Entry Delay	Trouble	Alarm Memory	Zones Bypassed (armed or not)	User or Installer Programming	Keypad Lockout
3	Status 3	Note 1*	Intellizone Delay	Fire Delay	Auto-Arm Delay	Access	Any Zone Tamper	Zone Low Battery	Fire Loop	Zone Supervision
4	Status 4	0	Chime Partition 1	Chime Partition 2	Chime Partition 3	Chime Partition 4	Siren Partition 1	Siren Partition 2	Siren Partition 3	Siren Partition 4
		1	N/A	N/A	N/A	N/A	Smoke Reset	Ground Start	Kissoff	N/A
		2	System Trouble	Comm. Trouble	Module Trouble	Network Trouble	N/A	N/A	N/A	Clock Loss
		3	AC Fail	Battery Fail	Aux. Limit	Bell Limit	Bell Absent	ROM Error	N/A	N/A
		4	TLM	Fail to Com1	Fail to Com2	Fail to Com3	Fail to Com4	Fail to ComPC	N/A	N/A
		5	Module Tamper	Module ROM Error	Module TLM	Module Fail to Com Phone#	Printer Fault	Module AC Fail	Module Battery Fail	Module Aux. Fail
		6	Missing Keypad	Any Module Missing	N/A	N/A	N/A	Global Network Failure	Network Overload	Module Network Com Fail
7	At the Selected Time	0	00:00	00:15	00:30	00:45	01:00	01:15	01:30	01:45
		1	02:00	02:15	02:30	02:45	03:00	03:15	03:30	03:45
		2	04:00	04:15	04:30	04:45	05:00	05:15	05:30	05:45
		3	06:00	06:15	06:30	06:45	07:00	07:15	07:30	07:45
		4	08:00	08:15	08:30	08:45	09:00	09:15	09:30	09:45
		5	10:00	10:15	10:30	10:45	11:00	11:15	11:30	11:45
		6	12:00	12:15	12:30	12:45	13:00	13:15	13:30	13:45
		7	14:00	14:15	14:30	14:45	15:00	15:15	15:30	15:45
		8	16:00	16:15	16:30	16:45	17:00	17:15	17:30	17:45
		9	18:00	18:15	18:30	18:45	19:00	19:15	19:30	19:45
		A	20:00	20:15	20:30	20:45	21:00	21:15	21:30	21:45
		B	22:00	22:15	22:30	22:45	23:00	23:15	23:30	23:45
8	Utility Keys	0	Keys 1 & 2	Keys 4 & 5	Keys 7 & 8	CLEAR & 0	Keys 2 & 3	Keys 5 & 6	Keys 8 & 9	0 & ENTER

First Digit	Event	Second Digit	Feature Select Programming							
			1	2	3	4	5	6	7	8
9	Access Granted	0	Door 01	Door 02	Door 03	Door 04	Door 05	Door 06	Door 07	Door 08
		1	Door 09	Door 10	Door 11	Door 12	Door 13	Door 14	Door 15	Door 16
		2	Door 17	Door 18	Door 19	Door 20	Door 21	Door 22	Door 23	Door 24
		3	Door 25	Door 26	Door 27	Door 28	Door 29	Door 30	Door 31	Door 32
	User Code Entered	8	Code 01	Code 02	Code 03	Code 04	Code 05	Code 06	Code 07	Code 08
		9	Code 09	Code 10	Code 11	Code 12	Code 13	Code 14	Code 15	Code 16
		A	Code 17	Code 18	Code 19	Code 20	Code 21	Code 22	Code 23	Code 24
		B	Code 25	Code 26	Code 27	Code 28	Code 29	Code 30	Code 31	Code 32
		C	Code 33	Code 34	Code 35	Code 36	Code 37	Code 38	Code 39	Code 40
		D	Code 41	Code 42	Code 43	Code 44	Code 45	Code 46	Code 47	Code 48
		E	Code 49	Code 50	Code 51	Code 52	Code 53	Code 54	Code 55	Code 56
		F	Code 57	Code 58	Code 59	Code 60	Code 61	Code 62	Code 63	Code 64
A	Arming	0	Code 01	Code 02	Code 03	Code 04	Code 05	Code 06	Code 07	Code 08
		1	Code 09	Code 10	Code 11	Code 12	Code 13	Code 14	Code 15	Code 16
		2	Code 17	Code 18	Code 19	Code 20	Code 21	Code 22	Code 23	Code 24
		3	Code 25	Code 26	Code 27	Code 28	Code 29	Code 30	Code 31	Code 32
		4	Code 33	Code 34	Code 35	Code 36	Code 37	Code 38	Code 39	Code 40
		5	Code 41	Code 42	Code 43	Code 44	Code 45	Code 46	Code 47	Code 48
		6	Code 49	Code 50	Code 51	Code 52	Code 53	Code 54	Code 55	Code 56
		7	Code 57	Code 58	Code 59	Code 60	Code 61	Code 62	Code 63	Code 64
	Disarming	8	Code 01	Code 02	Code 03	Code 04	Code 05	Code 06	Code 07	Code 08
		9	Code 09	Code 10	Code 11	Code 12	Code 13	Code 14	Code 15	Code 16
		A	Code 17	Code 18	Code 19	Code 20	Code 21	Code 22	Code 23	Code 24
		B	Code 25	Code 26	Code 27	Code 28	Code 29	Code 30	Code 31	Code 32
		C	Code 33	Code 34	Code 35	Code 36	Code 37	Code 38	Code 39	Code 40
		D	Code 41	Code 42	Code 43	Code 44	Code 45	Code 46	Code 47	Code 48
		E	Code 49	Code 50	Code 51	Code 52	Code 53	Code 54	Code 55	Code 56
		F	Code 57	Code 58	Code 59	Code 60	Code 61	Code 62	Code 63	Code 64
B	Zone is OK	0	Zone 01	Zone 02	Zone 03	Zone 04	Zone 05	Zone 06	Zone 07	Zone 08
		1	Zone 09	Zone 10	Zone 11	Zone 12	Zone 13	Zone 14	Zone 15	Zone 16
		2	Zone 17	Zone 18	Zone 19	Zone 20	Zone 21	Zone 22	Zone 23	Zone 24
		3	Zone 25	Zone 26	Zone 27	Zone 28	Zone 29	Zone 30	Zone 31	Zone 32
		4	Zone 33	Zone 34	Zone 35	Zone 36	Zone 37	Zone 38	Zone 39	Zone 40
		5	Zone 41	Zone 42	Zone 43	Zone 44	Zone 45	Zone 46	Zone 47	Zone 48
	Zone is Open	8	Zone 01	Zone 02	Zone 03	Zone 04	Zone 05	Zone 06	Zone 07	Zone 08
		9	Zone 09	Zone 10	Zone 11	Zone 12	Zone 13	Zone 14	Zone 15	Zone 16
		A	Zone 17	Zone 18	Zone 19	Zone 20	Zone 21	Zone 22	Zone 23	Zone 24
		B	Zone 25	Zone 26	Zone 27	Zone 28	Zone 29	Zone 30	Zone 31	Zone 32
		C	Zone 33	Zone 34	Zone 35	Zone 36	Zone 37	Zone 38	Zone 39	Zone 40
		D	Zone 41	Zone 42	Zone 43	Zone 44	Zone 45	Zone 46	Zone 47	Zone 48

First Digit	Event	Second Digit	Feature Select Programming							
			1	2	3	4	5	6	7	8
C	Auto Zone Shutdown	0	Zone 01	Zone 02	Zone 03	Zone 04	Zone 05	Zone 06	Zone 07	Zone 08
		1	Zone 09	Zone 10	Zone 11	Zone 12	Zone 13	Zone 14	Zone 15	Zone 16
		2	Zone 17	Zone 18	Zone 19	Zone 20	Zone 21	Zone 22	Zone 23	Zone 24
		3	Zone 25	Zone 26	Zone 27	Zone 28	Zone 29	Zone 30	Zone 31	Zone 32
		4	Zone 33	Zone 34	Zone 35	Zone 36	Zone 37	Zone 38	Zone 39	Zone 40
		5	Zone 41	Zone 42	Zone 43	Zone 44	Zone 45	Zone 46	Zone 47	Zone 48
	Zone Bypass (when system is armed)	8	Zone 01	Zone 02	Zone 03	Zone 04	Zone 05	Zone 06	Zone 07	Zone 08
		9	Zone 09	Zone 10	Zone 11	Zone 12	Zone 13	Zone 14	Zone 15	Zone 16
		A	Zone 17	Zone 18	Zone 19	Zone 20	Zone 21	Zone 22	Zone 23	Zone 24
		B	Zone 25	Zone 26	Zone 27	Zone 28	Zone 29	Zone 30	Zone 31	Zone 32
		C	Zone 33	Zone 34	Zone 35	Zone 36	Zone 37	Zone 38	Zone 39	Zone 40
		D	Zone 41	Zone 42	Zone 43	Zone 44	Zone 45	Zone 46	Zone 47	Zone 48
D	Zone Fault (Tamper/Fire Loop)	0	Zone 01	Zone 02	Zone 03	Zone 04	Zone 05	Zone 06	Zone 07	Zone 08
		1	Zone 09	Zone 10	Zone 11	Zone 12	Zone 13	Zone 14	Zone 15	Zone 16
		2	Zone 17	Zone 18	Zone 19	Zone 20	Zone 21	Zone 22	Zone 23	Zone 24
		3	Zone 25	Zone 26	Zone 27	Zone 28	Zone 29	Zone 30	Zone 31	Zone 32
		4	Zone 33	Zone 34	Zone 35	Zone 36	Zone 37	Zone 38	Zone 39	Zone 40
		5	Zone 41	Zone 42	Zone 43	Zone 44	Zone 45	Zone 46	Zone 47	Zone 48
	RF Zone Fault (Low Battery Supervision)	8	Zone 01	Zone 02	Zone 03	Zone 04	Zone 05	Zone 06	Zone 07	Zone 08
		9	Zone 09	Zone 10	Zone 11	Zone 12	Zone 13	Zone 14	Zone 15	Zone 16
		A	Zone 17	Zone 18	Zone 19	Zone 20	Zone 21	Zone 22	Zone 23	Zone 24
		B	Zone 25	Zone 26	Zone 27	Zone 28	Zone 29	Zone 30	Zone 31	Zone 32
		C	Zone 33	Zone 34	Zone 35	Zone 36	Zone 37	Zone 38	Zone 39	Zone 40
		D	Zone 41	Zone 42	Zone 43	Zone 44	Zone 45	Zone 46	Zone 47	Zone 48
E	Fire or Burglar Alarms	0	Zone 01	Zone 02	Zone 03	Zone 04	Zone 05	Zone 06	Zone 07	Zone 08
		1	Zone 09	Zone 10	Zone 11	Zone 12	Zone 13	Zone 14	Zone 15	Zone 16
		2	Zone 17	Zone 18	Zone 19	Zone 20	Zone 21	Zone 22	Zone 23	Zone 24
		3	Zone 25	Zone 26	Zone 27	Zone 28	Zone 29	Zone 30	Zone 31	Zone 32
		4	Zone 33	Zone 34	Zone 35	Zone 36	Zone 37	Zone 38	Zone 39	Zone 40
		5	Zone 41	Zone 42	Zone 43	Zone 44	Zone 45	Zone 46	Zone 47	Zone 48
	Fire or Burglar Restore	8	Zone 01	Zone 02	Zone 03	Zone 04	Zone 05	Zone 06	Zone 07	Zone 08
		9	Zone 09	Zone 10	Zone 11	Zone 12	Zone 13	Zone 14	Zone 15	Zone 16
		A	Zone 17	Zone 18	Zone 19	Zone 20	Zone 21	Zone 22	Zone 23	Zone 24
		B	Zone 25	Zone 26	Zone 27	Zone 28	Zone 29	Zone 30	Zone 31	Zone 32
		C	Zone 33	Zone 34	Zone 35	Zone 36	Zone 37	Zone 38	Zone 39	Zone 40
		D	Zone 41	Zone 42	Zone 43	Zone 44	Zone 45	Zone 46	Zone 47	Zone 48
F	Module Troubles	0	Network Fault	Module Tamper	ROM Error	Module TLM	Fail to Com	Printer Fault	AC Fail	Battery Fail
		1	Aux. Output Fail	N/A	N/A	N/A	N/A	N/A	N/A	N/A
		8	Network Fault Restore	Module Tamper Restore	ROM Error Restore	Module TLM Restore	Fail to Com. Restore	Printer Fault Restore	AC Fail Restore	Battery Fail Restore
		9	Aux. Fail	N/A	N/A	N/A	N/A	N/A	N/A	N/A

SYSTEM SETTINGS & COMMANDS

12.1 HARDWARE RESET

Performing a hardware reset will set all programmable sections from **[001]** to **[718]** to default values, including the Installer Code and System Master Code. Only the Panel ID, PC Password and Event Buffer will not be reset.

- 1) Make sure the Installer Code Lock is disabled (see section 12.4)
- 2) Remove the battery and AC power from the control panel.
- 3) Set the RESET jumper to on by placing a jumper on the reset pins of the control panel.
- 4) Re-connect the AC power and the battery to the control panel.
- 5) Wait 10 seconds and remove the jumper.

12.2 SOFTWARE RESET

Performing a software reset will set certain parameters to default values or program certain sections with a set of pre-defined values. To do so:

- 1) Make sure the RESET jumper on the control panel is on.
- 2) Enter *Panel Programming Mode* (see section 3.1).
- 3) Enter the 3-digit **[SECTION]** corresponding to the software reset you wish to perform:

Section **[970]**

Entering this section will reset all programmable sections from **[001]** to **[896]** to default values. Only the Event Buffer, Installer Code, System Master Code, Panel ID and PC Password will not be reset.

Section **[974]**

Access Control reset sections from **[301]** to **[392]**.

Section **[975]**

Entering this section will reset all Zone and Keyswitch programming sections from **[001]** to **[156]** to default values.

Section **[976]**

Entering this section will reset all programmable timers in sections **[200]** to **[450]** to default values.

Section **[977]**

Entering this section will reset sections from **[500]** to **[522]** to default values.

Section **[978]**

Entering this section will reset all communication sections from **[523]** to **[718]** (except **[537]**) to default values.

Section **[979]**

Entering this section will reset all user code sections from **[801]** to **[896]** to default values.

12.3 BATTERY CHARGE CURRENT

SECTION **[503]: OPTION **[6]****

Option **[6]** ON = Battery Charge Current: 700mA (minimum 40VA transformer)

Option **[6]** OFF = Battery Charge Current: 350mA

12.4 INSTALLER CODE LOCK

SECTION **[990]**

Enter 147 into section **[990]** to lock all programming. When 147 is programmed in section **[990]**, performing a hardware reset as described in section 12.1 will not affect the current panel settings. To remove the Installer Lock, enter 000 into section **[990]**. (Default: Unlocked)

12.5 PARTITIONING

SECTION **[500]: OPTIONS **[1]** TO **[4]****

The Digiplex Control Panel can provide your system with up to four completely independent partitions. Most features and options in the Digiplex System can be independently set for each partition such as Event Reporting, Entry/Exit Delay, Bell Squawk, One-touch Arming, Panic Alarms and many more. All zones, keyswitch zones, user codes and system modules are assigned to specific partitions, making this a true partitioned system. In section **[500]**, enable the option(s) that correspond to the desired partition(s). Where options **[1]** to **[4]** represent partitions 1 through 4.

12.5.1 Panel Partition Assignment

SECTION **[450]**

The control panel will report system events as originating from the partitions enabled in this section. The System Troubles (i.e. AC Failure, TLM Failure, etc.) can only be viewed through the partitions enabled in this section.

00 = All enabled partitions (see section **[500]**)

01 = Control Panel installed in Partition 1

02 = Control Panel installed in Partition 2

03 = Control Panel installed in Partition 3

04 = Control Panel installed in Partition 4

12.6 INSTALLER FUNCTION KEYS

Press and hold the **[0]** key and key in the **[INSTALLER CODE]** to access the following function keys.

[STAY]: TEST REPORT

Sends the *Test Report* report code programmed in section **[717]** to the central station.

[FORCE]: CALL WINLOAD

Will dial the PC telephone number programmed in section **[560]** to communicate with a computer using WinLoad.

[ARM]: ANSWER WINLOAD

Will force the control panel to answer a call made by the Central Monitoring Station that is using WinLoad.

[DISARM]: CANCEL COMMUNICATION

Pressing this function key cancels all communication with the Central Station or WinLoad until the next reportable event.

[MEM]: INSTALLER TEST MODE

The Installer Test Mode will allow you to perform walk tests where the bell or siren will squawk to indicate opened zones. Press **[MEM]** again to exit. Partitions cannot be armed if the Installer Test Mode is enabled.

[TRBL]: MODULE SCAN

This feature instructs the control panel to verify the status of the modules connected to the network. The control panel will fix any problems with the internal organization of the modules in the control panel. The LCD Keypads will display the serial number of each module that has been connected to the network.

[ACC]: NETWORK VOLTMETER

For LCD Keypads (DGP2-641/DGP2-641AC) only.

To verify if the network is supplying sufficient power, press and hold the [0] key, enter the [INSTALLER CODE] and press the [ACC] key on the keypad. A reading of 9.2V indicates that the voltage is too low. The voltage may drop during the control panel battery test (see section 2.4.1).

12.7 SYSTEM DATE & TIME

SECTION [502]: OPTION [6]

The System Date and Time is programmed through the User Menu, please refer to Clock Loss section 16.7.

12.7.1 Daylight Savings Time

By enabling option [6] in section [502], the control panel will automatically adjust the system's clock (time) for daylight saving changes. At 2:00AM on the first Sunday of a full weekend in April, the control panel will add one hour to the programmed time (clock). At 2:00AM on the last Sunday of a full weekend in October, the control panel will subtract one hour from the programmed time (clock).

12.8 SHABBAT FEATURE

SECTION [522]: OPTION [4]

With option [4] on, all addressable detection devices and keypads in the system will no longer display any system status through the LCD and/or LEDs between noon (12:00PM) Friday and midnight (12:00AM) Saturday. Therefore, normal operation will be re-instated Sunday morning at 12:00:01AM.

During the Shabbat period:

- the LCD keypads only display the date and time
- the backlight is disabled
- the LED indicators on all addressable detection devices and keypads in the system are disabled

If required, a user can access all the usual commands and features during the Shabbat period by pressing a key or, if Confidential Mode is enabled in the keypad, by entering their access code. When no actions have occurred for two minutes, the Shabbat Feature will re-activate.

12.9 MODULE RESET

SECTION [951]

To reset a module that is connected to the network to its default values, key in the module's serial number into section [951].

12.10 LOCATE MODULE

SECTION [952]

If you wish to locate a specific module (e.g. detector, zone expansion module, etc.) connected to the network, key in the

module's serial number into section [952]. The green LOCATE LED on the module will begin to flash until the serial number is re-entered into section [952] or the appropriate tamper or unlocate switch on the module is pressed.

12.11 MODULE PROGRAMMING

SECTION [953]

All modules connected to the network are programmed through the control panel. Therefore, if you wish to program a module, enter section [953] to enter *Module Programming Mode* (see section 3.2) and key in the module's serial number. At this point, any sections entered will be those of the selected module. For details on how to program the modules, refer to the module's Installer's Guide or the module's *Programming Guide*. To exit this mode, press the [CLEAR] key until you are in Normal Mode.

12.12 MODULE BROADCAST

SECTION [954]

This feature allows you to copy the contents of all programming sections from one module to one or more of the same type of module. In section [954], key in the serial number of the source module, then enter the serial numbers of all the destination modules you wish to program and press [ACC].



The Module Broadcast feature will only work when a module is broadcasting its data to a module or to modules of the same type and model number. For example, an APR-PRT1 (Printer Module) cannot broadcast to an APR3-PRT1. Likewise, a DGP module cannot broadcast to a DGP2 module.

For example:

You've completed the programming of a zone expansion module (sn#30540033) and you wish to program another two zone expansion modules (sn#30540075 and sn#30412100) with the same settings and options:

- 1) Press and hold the [0] key
- 2) Key in the Installer Code
- 3) Enter [954]
- 4) Enter 30540033, 30540075, and 30412100
- 5) Press [ACC].

The control panel will automatically copy the contents of 30540033 into the other two zone expansion modules.

12.13 REMOVE MODULE

SECTION [955]

After entering section [955], the control panel will scan all modules connected to the network. If any missing modules are detected (i.e. detector removed from the network) during this scan, the control panel will erase the module's serial number and remove the module from the control panel's memory.

12.14 SERIAL NUMBER VIEWING

SECTION [900]

This feature allows you to view the serial number of the control panel as well as the serial numbers of all modules connected to the network.

With the LCD Keypad: After entering section **[900]**, the keypad will display the eight-digit serial number of the control panel. Use the **[▲]** and **[▼]** keys to scroll through the serial number of each module connected to the network.

With the LED Keypads: After entering section **[900]**, the serial number of the control panel will illuminate one number at a time as you press the **[▲]** key ([10] LED represents zero). The keypad will emit a confirmation beep to indicate that it is now displaying the serial number of the next module connected to the network.

12.15 POWER SAVE MODE

SECTION [504]: OPTIONS [4]

When the control panel is running on the backup battery (no AC), the control panel can set all keypads into a “sleep mode” or Power Save Mode. In Power Save Mode the keypad's backlight and LEDs will be disabled until a key is pressed, an alarm occurs or an Entry Delay is triggered.

12.16 AUTO TROUBLE SHUTDOWN

SECTION [218]

If, in a 24-hour period, a trouble has occurred more than the number of times programmed in section **[218]**, the control panel will no longer report this trouble. Enter a value (001 to 015, 000 = disabled) into section [218]. Please note that each trouble has its own counter. This counter is reset every day at midnight or when a *Module Scan* is performed (see section 12.6). Also, note that it cannot be set to more than 15.

12.17 NO AC FAIL DISPLAY

SECTION [503]: OPTION [7]

With option **[7]** in section **[503]** enabled, the control panel will not display the AC Failure as a trouble. This means that when an AC Failure occurs when this option is on:

- the AC LED will extinguish
- the trouble will not appear in the Trouble Display
- the keypad will not beep to indicate the trouble
- the AC Failure report code will be reported.

ACCESS CODES

The Digiplex control panel supports 95 User Access Codes, 1 System Master Code, and 1 Installer Code.

13.1 INSTALLER CODE

SECTION [800]

(Default: 000000) The Installer Code is used to enter the control panel's programming mode, which allows you to program all the features, options and commands of the control panel and any modules connected to the network. **The Installer Code can program the User Code Options and the Partition Assignment, but cannot program the personal identification numbers.** The Installer Code is six digits in length where each digit can be any value from 0 to 9.

To change the Installer Code:

- 1) Press and hold [0]
- 2) Enter [INSTALLER CODE]
- 3) Key in [800]
- 4) Enter new 6-digit [INSTALLER CODE]

13.2 ACCESS CODE LENGTH

SECTION [504]: OPTIONS [2] AND [3]

Access codes can be between 1 and 6 digits in length. When programming access codes with less than 6 digits, press the [ENTER] key. When you change the User Access Code Length from 4 digits to 6 digits, the control panel will automatically add the last 2 digits by using the first 2 digits. For example, if your Access Code is 1234 and you switch to 6 digits the code will become 123412. When you change the Access Code Length from 6 digits to 4 digits, the control panel will automatically remove the last 2 digits.

[2]	[3]	Option
Off	Off	4-digit Access Codes
Off	On	6-digit Access Codes
On	Off	Same as On/On
On	On	Flexible Access Codes

13.3 SYSTEM MASTER CODE

(Default: 123456) With the System Master Code a user can use any of the available arming methods with access to all partitions and can program all User Access Codes, User Options, Partition Assignments, and Access Control Options.

Each digit in the System Master Code can be any value from 0 to 9. The length of the System Master Code is determined by the Access Code Length feature (see section 13.2). The System Master Code cannot be set to less than 4 digits in length.

13.3.1 System Master Code Reset

SECTION [950]

To reset the System Master Code to its default (123456):

- Set the RESET jumper to on by placing a jumper on the reset pins of the control panel
- Use the Installer Code to enter section [950]



Do not remove the power from the control panel.

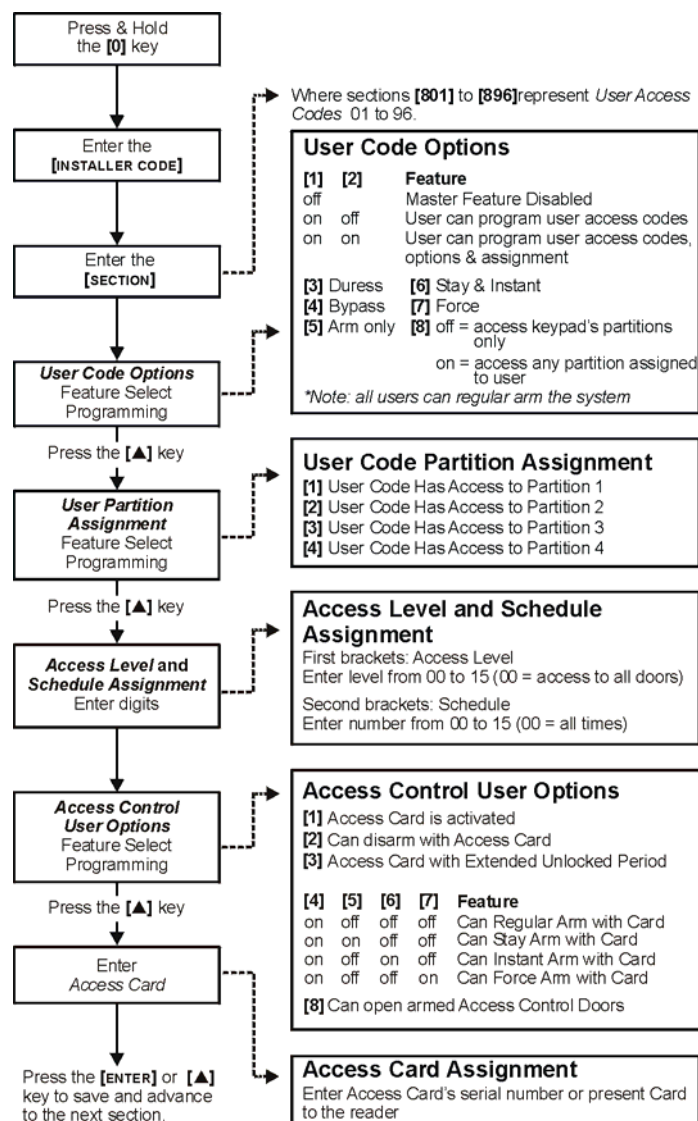
13.4 PROGRAMMING ACCESS CODES

Sections [801] to [896]

In section [801] the installer can program the System Master Code with an Access Card's serial number and change the Access Card's arming method (see section 13.7).

In sections [802] to [896], the Installer Code can program the User Code Options, Partition Assignment, and Access Control Options, but cannot program the user code for the System Master Code or the User Access Codes. To program the User Access Codes, refer the users to the appropriate User Manual: LCD Keypad User's Manual and LED Keypads User's Manual. If no partition assignment is selected, the User Access Code will **only** be able to activate PGMs.

Figure 13-1: Programming User Access Codes



13.5 USER OPTIONS

The User Options define how each User Access Code can arm or disarm the system. Regardless of these settings, all users can Regular Arm (see section 16.1) their assigned partitions and all users, except those with the *Arm Only* option (see section 13.5.4), can disarm an assigned partition. Select one or more of the options described in the following sub-sections for each User Access Code as shown in Figure 13-1 on page 40. The System Master Code or a User Access Code with the Master Feature enabled can also program the User Options using a different programming method. To program the User Access Codes, refer the users to appropriate User Manual: LCD Keypad User's Manual or LED Keypads User's Manual.

13.5.1 Master Feature

SECTIONS [802] TO [896]: OPTIONS [1] AND [2]

[1]	[2]	Option
Off	Off	Master Feature Disabled
Off	On	Master Feature Disabled
On	Off	Users can create or modify User Access Codes that have the same partition assignment.
On	On	Users can create or modify User Access Codes with the same partition assignment and program the User Options and Partition Assignment (assigns only partitions the Master Feature Code has access to).

13.5.2 Duress

SECTIONS [802] TO [896]: OPTION [3]

When a user is forced to arm or disarm their system, entering a Duress enabled User Access Code (option [3] On) will arm or disarm the system and, if programmed, will immediately transmit a silent alarm to the Central Station.

13.5.3 Bypass Programming

SECTIONS [802] TO [896]: OPTION [4]

The User Access Code with option [4] enabled can program bypass entries as described in section 16.2.

13.5.4 Arm Only

SECTIONS [802] TO [896]: OPTION [5]

The User Access Code with option [5] enabled can arm assigned partitions, but cannot disarm any partitions. The type of arming is determined by the other User Options selected. Please note that with the Arm Only option, the user who just armed the system can cancel arming by re-entering the same User Access Code during the Exit Delay.

13.5.5 Stay & Instant Arming

SECTIONS [802] TO [896]: OPTION [6]

The User Access Code with option [6] enabled, can Stay Arm or Instant Arm (see section 16.1) assigned partitions.

13.5.6 Force Arming

SECTIONS [802] TO [896]: OPTION [7]

The User Access Code with option [7] enabled will be able to Force Arm assigned partitions (see section 16.1).

13.5.7 User Menu Access Conditions

SECTIONS [802] TO [896]: OPTION [8]

This feature will govern which partitions users have access to when entering their access codes. With option [8] on, the control panel

will grant access to all partitions assigned to the User Access Code. With option [8] off, the control panel will only grant access to partitions that have been assigned to both the User Access Code and the keypad.

13.6 USER PARTITION ASSIGNMENT

SECTIONS [802] TO [896]: OPTIONS [1] TO [4]

Each of the 95 User Access Codes can be assigned to one or more partitions. A user can only arm, disarm and view status of the partitions assigned to their User Access Codes. Select one or more of the partitions for each User Access Code as shown in Figure 13-1 on page 40. If no partition assignment is selected, the User Access Code will **only** be able to activate PGMs. The System Master Code or a user with the Master Feature enabled can also program the User Partition Assignment using a different method of programming (see section 16.4).

13.7 ACCESS CONTROL

SECTIONS [801] TO [896]

In addition to the User Access Code options, the following options can be programmed when Access Control is enabled on the Digiplex system: Access Level, Schedule, Access User Options, and Access Card.



The System Master Code and User Access Codes with the Full Master feature enabled can also program the Access Level, Schedule, Access User Options, and Access Card on User Access Codes.



The System Master Code in section [801] has access to all doors all the time. Only the card's serial number and the choice of arming method can be changed. If the other options are changed, the System Master Code will revert to its original programming.

13.7.1 Access Level Assignment

SECTIONS [802] TO [896]: LEVEL & SCHEDULE SCREEN, FIRST BRACKETS

Enter the two-digit Access Level number (00 to 15) to be assigned to that User Access Code. Access Levels are defined in the sections [341] to [355] (see section 14.6). An Access Level is a combination of Access Doors that a User Access Code assigned to that level will be able to open. Access Level [00] will permit access to all Access Doors (unrestricted Access Level).

13.7.2 Schedule Assignment

SECTIONS [802] TO [896]: LEVEL & SCHEDULE SCREEN, SECOND BRACKETS

Enter the two-digit Schedule number (00 to 15) to be assigned to that User Access Code. Schedules determine the hours, days, and holidays that a User Access Code will be allowed to open Access Doors. The Schedules are defined in the sections [361] to [375] (see section 14.7). Schedule [00] will permit access at all times (unrestricted hours and days).

13.7.3 Activate Card for Access Control

SECTIONS [802] TO [896]: ACCESS OPTION SCREEN, OPTION [1]
Option [1] ON = The Access Card is activated and can be used when the Access Control is enabled.
Option [1] OFF = The User Access Code can be used with the Digiplex alarm system, but cannot use the Access Control features. This can be used to disable a lost or stolen card **without** deleting the User Access Code.

13.7.4 Disarm with Access Card

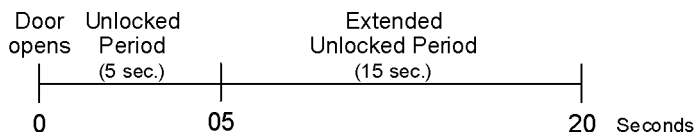
SECTIONS [802] TO [896]: ACCESS OPTION SCREEN, OPTION [2]
When the partition assigned to an Access Door (see section 14.4) is armed, it can be disarmed and unlocked upon presentation of a valid Access Card to the reader. For an Access Card to be valid, it must be presented during its assigned Schedule, within its assigned Access Level and be assigned to the keypad's assigned partitions depending on the Door Access Mode (see section 14.5). Codes assigned with the "Arm Only" User Option will not be able to disarm with the card.
Option [2] ON = The Access Card can disarm partitions.
Option [2] OFF = The Access Card cannot disarm partitions.

13.7.5 Card with Extended Unlocked Period

SECTIONS [802] TO [896]: ACCESS OPTION SCREEN, OPTION [3]
Each Access Control Keypad is programmed with a Door Unlocked Period and a Door Unlocked Period Extension. The Door Unlocked Period is the time the door can remain unlatched after access is granted or after a Request for Exit is received. The Door Unlocked Period Extension is the amount of time added to the Door Unlocked Period. For more details refer to the appropriate *Digiplex Module Reference & Installation Manual*.

When Card with Extended Unlocked Period is enabled, the two time periods are added together to allow extra time for the user to open the Access Door, which may be useful for seniors and for the physically challenged. Access is only granted during the card's assigned Schedule and to doors programmed in its Access Level.
Option [3] ON = Extended Unlocked Period is enabled on card
Option [3] OFF = Extended Unlocked Period is disabled on card

Example:



13.7.6 Arming with Access Card

SECTIONS [802] TO [896]: ACCESS OPTION SCREEN, OPTIONS [4], [5], [6], AND [7]
An Access Card can be programmed to arm the partition(s) assigned to the door when the valid card is presented to the reader twice within approximately 5 seconds while the door remains closed. For an Access Card to be valid, it must be presented during its assigned Schedule, within its assigned Access Level and be assigned to the keypad's assigned partitions depending on the Door Access Mode (see section 14.5). The arming method is determined by turning ON or OFF one of the options from [5] to [7].

NO ARMING WITH CARD

Option [4] OFF = Arming with Access Card is disabled.

REGULAR ARMING WITH CARD

Option [4] ON and Options [5], [6], & [7] OFF = The Access Card can Regular Arm partitions (see section 16.1).

STAY ARMING WITH CARD

Options [4] and [5] ON and Options [6] and [7] OFF = The Access Card can Stay Arm the partitions (see section 16.1).

INSTANT ARMING WITH CARD

Options [4] and [6] ON and Options [5] and [7] OFF = The Access Card can Instant Arm the partitions (see section 16.1).

FORCE ARMING WITH CARD

Options [4] and [7] ON and Options [5] and [6] OFF = The Access Card can Force Arm the partitions (see section 16.1).

13.7.7 Access to Armed Access Doors

SECTIONS [802] TO [896]: ACCESS OPTION SCREEN, OPTION [8]
An Access Door can be assigned to a zone in Digiplex so it can be protected by the security system as well (see section 14.4). When a valid Access Card with this feature enabled is presented to an armed door, access will be granted and the Entry Delay will begin. When this option is enabled, extra security is provided since a user **must** enter a User Access Code to disarm the area. Access is only granted during the card's assigned Schedule and to doors programmed in its Access Level. For User Access Codes assigned with the "Arm Only" User Option, option [8] should remain off since they cannot disarm the partition(s).

For this feature to function properly, Option [2] Disarm with Access Card must be disabled. If option [2] is enabled, access will be granted and the partition(s) will be disarmed without entering the User Access Code.

Option [8] ON = Access to armed doors is granted

Option [8] OFF = Access to armed doors is denied

13.7.8 Access Card Assignment

SECTIONS [801] TO [896]: ACCESS CARD SCREEN
The Access Card is activated by assigning its serial number to the User Access Code. This system supports only the proximity cards by Position Technology. Either enter the serial number manually or present the Access Card to the keypad's reader and its serial number will register automatically.

13.8 MULTIPLE ACTION FEATURE

SECTION [504]: OPTION [1]

By enabling option [1] in section [504], users will remain in the User Menu after entering their access code. This allows users to perform more than one action without having to re-enter their access code. With option [1] off in section [504], the control panel will exit the User Menu after every action.

ACCESS CONTROL

Access control is an industry term for a system that monitors and regulates the passage into and out of protected areas. With access control, you can identify who accesses a site and limit the days and times that specific people can enter and exit that site.

Each door in the access control system is equipped with a reader, an access control keypad, a request-for-exit motion detector, a door contact and an electronic door strike. These devices work together with the control panel to unlock the door only for authorized personnel at authorized periods of time.

Each person who is authorized to access the protected area is issued a card. The card is assigned to a User Access Code and programmed with an Access Level (see section 14.6) and a Schedule (see section 14.7). When a card is presented to the reader, the control panel will determine whether or not to unlock the door depending on if the card is allowed to open that door (Access Level) and if the card is permitted at that particular time and day (Schedule).

Access Control features can only be enabled and programmed through either the LCD Keypad (DGP2-641) or the Access Control Keypad (DGP2-641AC). The general Access Control options are programmed in the control panel. Specific options for each door are programmed through the LCD or Access Control keypads (see the appropriate *Digiplex Module Reference & Installation Manual*).

In order to program the Access Control features in the Digiplex Control Panel, you must enter Panel Programming Mode:

- Step 1: Press and hold the **[0]** key.
- Step 2: Enter the **[INSTALLER CODE]** (by default 000000)
- Step 3: Panel Programming Mode: Enter desired 3-digit **[SECTION]**
- Step 4: Enter the required **[DATA]**.

14.1 PROGRAMMING ACCESS CONTROL OVERVIEW

The following is the minimum required to program an Access Control system. Depending on the requirements of the installation, some of the other features explored in this chapter may be necessary.

- Step 1: Enable Access Control in section **[537]** option **[1]**
- Step 2: Assign the Keypads to Doors in sections **[301]** to **[332]**
- Step 3: Create the Access Levels in sections **[341]** to **[355]**
- Step 4: Set the Holidays in sections **[381]** to **[392]**
- Step 5: Create the Schedules in sections **[361]** to **[375]**
- Step 6: Program User Access Code with Access Control Options in sections **[801]** to **[896]**

14.2 COMMON ACCESS CONTROL TERMS

ACCESS ALARM:

An audible or silent warning generated by the reader to indicate that a protected door has not closed within the programmed time allowed or that a protected door was opened without an "Access Granted" or "Request for Exit" signal.

ACCESS CARD:

A tag assigned to a User Access Code used to identify the user to the Access Control system. By presenting the tag to a reader, the system can verify whether the tag is valid.

DOOR LEFT OPEN:

Each Access Door is programmed with a period of time it is allowed to remain open. Once the door has been open past this time limit, an Access Alarm will be triggered.

FORCED DOOR:

If a protected door was opened without an "Access Granted" or "Request for Exit" signal, a silent or audible Access Alarm can be triggered.

READER:

An Access Control device (Posiprox CR-R880) normally located near a protected door that serves to relay the information from an Access Card presented to it to the control panel.

REQUEST FOR EXIT:

When a REX device (Parado 460) installed above an Access Door within a protected area detects movement, it sends a signal to the panel to permit a user to leave the protected area.

VALID CARD:

An Access Card presented to a reader during its assigned Schedule and within its assigned Access Level.

14.3 ENABLE ACCESS CONTROL

SECTION [537]: OPTION [1]

When Access Control is enabled, the control panel and the keypads must be programmed for the feature to function properly.

Option **[1]** ON = Access Control is enabled.

Option **[1]** OFF = Access Control feature is disabled. (default)

14.4 ASSIGNING THE KEYPAD TO A DOOR

SECTIONS [301] TO [332]

Each door to be monitored and controlled requires an Access Control Keypad (DGP2-641AC). The keypad is assigned to the door through the keypad's serial number in these sections. You can assign up to 32 Access Control Keypads in a Digiplex system. The Access Doors are then combined to determine the Access Levels. If you want the Access Doors also to be linked to the alarm system, assign the keypad zone input to a zone in the control panel (see section 4).

14.5 DOOR ACCESS MODE

SECTION [340]

Although the keypad can be programmed to display the status of various partitions, the Access Door can be assigned to one or more partition(s) in the alarm system. This means that the actions performed with the Access Card will be directly linked to the partition(s) assigned to that door. For more details refer to *Partition Assignment* and *Assigning Doors to Partitions* in the appropriate *Digiplex Module Reference & Installation Manual*.

Each door can be programmed to grant access only to cards assigned to **all** the door's assigned partitions ("AND" Door Access Mode) **or** to cards assigned to **at least one** of the door's partitions ("OR" Door Access Mode). For an "AND" Access Door to grant access or to arm all its assigned partitions, the Access Card must be assigned to all the door's assigned partitions. To access an "OR" Access Door, the Access Card must be assigned to at least one partition assigned to the door. An "OR" door will arm or disarm only the partitions that it has in common with the card.

Section [340] consists of four screens of eight options each. Each option represents an Access Door. Enable the option corresponding to the door to be set in "OR" Door Access Mode. Options that remain disabled represent doors set in the "AND" Door Access Mode. For example, if option [2] in the Second Screen is enabled in section [340], Door 10 will use the "OR" Door Access Mode.

Option ON = "OR" Door Access Mode
Option OFF = "AND" Door Access Mode (default)

14.6 ACCESS LEVELS

SECTIONS [341] TO [355]

Users will only be allowed access to the doors assigned in the Access Level programmed on their User Access Codes (see section 13.7.1). Each Access Level is a combination of the Access Doors that were assigned in sections [301] to [332]. You can program up to 15 different Access Levels (from 01 to 15). Level 00 allows the user access to all the Access Doors. Using *Feature Select Programming*, enable or disable options representing the desired doors. For example, if the options representing doors 01, 02, and 03 are enabled in section [341], any User Access Code or Access Card assigned to Level 01 will only have access to doors 01, 02, and 03.

14.7 SCHEDULES

SECTIONS [361] TO [375]

Schedules determine the hours, days, and holidays that users are permitted access. You can program up to 15 different Schedules (from 01 to 15). Schedule 00 allows the user access at all times. Each Schedule consists of two programmable time periods called Intervals that determine the time of day and which days the users will be granted access. When a schedule is programmed with "H", users will have access during the days programmed in the sections [381] to [392] (see section 14.8). Each user is assigned a Schedule through the User Access Code.

Program the Start Time and End Time according to the 24-hour clock within the same day. Use *Feature Select Programming* to set the options representing the Days.

Option	Day	Option	Day
[1]	Sunday (S)	[5]	Thursday (T)
[2]	Monday (M)	[6]	Friday (F)
[3]	Tuesday (T)	[7]	Saturday (S)
[4]	Wednesday (W)	[8]	Holidays (H)

For example, program Schedule 01 in section [361]:

- Interval A with Start time **07:00**, End time **16:00**, Days **M, T, W, T, and F**
- Interval B with Start time **10:00**, End time **17:00**, Days **S, S, and H**

Then, any User Access Code with this Schedule assigned will only be allowed access Monday to Friday from 7AM to 4PM and on Saturday, Sunday, and Holidays from 10AM to 5PM.

14.8 HOLIDAY PROGRAMMING

SECTIONS [381] TO [392]

Holiday Programming identifies the days that are considered holidays. When option [8] is enabled in sections [361] to [375], access is permitted during the programmed holidays.

Each section represents a month. Each section includes four groups of eight options that represent the days of the month. Use *Feature Select Programming* to enable the options representing the days to be designated as holidays. For example, if 1 and 2 are enabled in the fourth screen in section [392], then December 25 and 26 are designated as holidays. When [8] is enabled in sections [361] to [375], those users will have access according to their Schedule on December 25 and 26.

14.9 LOGGING ACCESS CONTROL EVENTS

14.9.1 Log Request For Exit In Event Buffer

SECTION [537]: OPTION [2]

When the REX device registers movement at the door, a Request for Exit (REX) event is generated (see section 14.2). The Control Panel can record the REX events generated from all the Access Doors in the system, but cannot report these events to the Monitoring Station. The events can be viewed through an Access Control Keypad by entering the *Event Record Display* (see section 16.8).

Option [2] ON = Record the REX events
Option [2] OFF = Do not record the REX events (default)



Since REX events can occur often, the Event Buffer may fill up quickly.

14.9.2 Log Door Left Open Restore In Event Buffer

SECTION [537]: OPTION [3]

The Door Left Open Interval is the time that a door can remain open after an Access Granted or a Request for Exit without generating an Access Alarm. If an Access Door is left open beyond its keypad's programmed Door Left Open Interval and then is closed, it can generate a Door Left Open Restore event in the Event Buffer. These events cannot be reported to the Monitoring Station, but they can be viewed through an Access Control Keypad by entering the *Event Record Display* (see section 16.8).

Option [3] ON = Record the Door Left Open Restore events
Option [3] OFF = Do not record the Door Left Open Restore events (default)

14.9.3 Log Door Forced Open Restore In Event Buffer

SECTION [537]: OPTION [4]

An Access Door is considered forced when its door contact is opened without the use of a valid Access Card or User Access Code or receiving a Request for Exit signal (see section 14.2).

If an Access Door is forced open then closed, it can generate a Door Forced Open Restore event in the Event Buffer. This event cannot be reported to the Monitoring Station, but it can be viewed through an Access Control Keypad (DGP2-641AC) by entering the *Event Record Display* (see section 16.8). To have the Door Forced Open Alarm reported to the Monitoring Station see section 14.10.1.

Option [4] ON = Record the Door Forced Open Restore events

Option [4] OFF = Do not record the Door Forced Open Restore events (default)

14.10 GLOBAL ACCESS DOOR FEATURES

14.10.1 Burglar Alarm On Forced Door

SECTION [537]: OPTION [5]

An Access Door can be assigned to a zone in the Digiplex security system to also be protected by the burglar alarm. If an armed Access Door is forced open (see section 14.2), it can send a signal to the control panel to trigger a burglar alarm and to report to the Monitoring Station. The burglar alarm is generated instantly regardless of the zone's definition (i.e. entry delay is ignored).

For this feature to function, the following must be done:

- Install a door contact (see appropriate *Digiplex Module Reference & Installation Manual*)
- Assign the Access Door to a zone (see section 4)
- Enable option [4] in section [537]: Log Door Forced Open Restore (optional) (see section 14.9)
- Enable option [5] in section [537]: Burglar Alarm on Forced Door (see section 14.10.1)

Option [5] ON = Burglar Alarm on Forced Door enabled

Option [5] OFF = Burglar Alarm on Forced Door disabled (default)

14.10.2 Skip Exit Delay When Arming With Access Card

SECTION [537]: OPTION [6]

When an Access Card is presented to a reader twice within approximately 5 seconds with the door closed, some or all the partitions (see section 14.5) assigned to the Access Door can arm with or without starting the Exit Delay. This feature is useful when the reader is outside the partition so the partition will be armed immediately.

Option [6] ON = The Exit Delay will not be triggered

Option [6] OFF = The Exit Delay will be triggered (default)

14.10.3 Door Access During Clock Loss

SECTION [537]: OPTION [8]

If the system registers a Clock Loss Trouble, the system will no longer be able to recognize the Schedules. Only the *System Master Code* and *User Access Codes* with the *Master* feature enabled can reset the clock when option [8] is enabled. To avoid a Clock Loss Trouble, the Digiplex Time Module (DGP2-TM1) can be installed on the control panel. Until the Clock is reset, the Access Control system can be programmed to grant access to:

Option [8] ON = only the System Master Code, User Access Codes with the Full Master feature enabled or User Access Codes with the Schedule 00

Option [8] OFF = all users regardless of their programmed Schedule (default)

15.1 ANSWERING MACHINE OVERRIDE

SECTION [451]

When using WinLoad to communicate remotely with an installation site that uses an answering machine or service, the Answering Machine Override must be programmed. Using WinLoad, call the installation site and on the second ring press the **[ENTER]** key on the keyboard to hang up or hang up manually. After hanging up, WinLoad will immediately call the installation site back or call the site back manually. The value (00 to 15 X 4 seconds) programmed in section **[451]** represents the delay period the control panel will wait between the first and second call. If the installation site is called back within the programmed delay period, the control panel will override the answering machine or service by picking-up the line on the first ring. To disable this option program 00 in section **[451]**. Also, see section 15.2.

Example: A security installation is using an answering machine set to answer after three rings and section [451] has been programmed with 10 (10 x 4 = 40 seconds). When you call the installation site with WinLoad the first time, wait two rings and press [ENTER] on the keyboard. WinLoad will immediately call the installation site back. If the second call is made within 40 seconds, the control panel will pick-up the line on the first ring. If it takes more than 40 seconds, the control panel will not answer on the first ring and the answering machine will answer after three rings.

15.2 RING COUNTER

SECTION [452]

The value (01 to 15, 00 = disabled) programmed in section **[452]** represents the number of rings the control panel will wait before picking-up the line. If the line is not answered after the number of programmed rings, the control panel will answer the call. The control panel resets the Ring Counter every 10 seconds. Therefore, if there is more than 10 seconds between each ring, the control panel will reset the counter on the next call. Also, see section 15.1.

15.3 PANEL IDENTIFIER

SECTION [555]

This four-digit code identifies the control panel to WinLoad before initiating upload or download. The control panel will verify if the panel identifier in WinLoad is the same. If the codes do not match, the control panel will not establish communication. Therefore, program the same Panel Identifier into both the Digiplex Control Panel and WinLoad. To program the Panel Identifier, key in the desired 4-digit hexadecimal number into section **[555]**.

15.4 PC PASSWORD

SECTION [556]

This four-digit password identifies the computer running the WinLoad software to the panel before beginning the download process. Program the same PC Password into both the Digiplex control panel and WinLoad. If the passwords do not match, WinLoad will not establish communication. To program the PC Password, enter the desired four-digit hexadecimal number into section **[556]**.

15.5 PC TELEPHONE NUMBER

SECTION [560]

The control panel will dial this number when trying to initiate communication with a computer using WinLoad. You can enter any digit from 0 to 9 and any special keys or functions (see Table 3, *Special Telephone Number Keys*, on page 28) up to a maximum of 32 digits into section **[560]**.



For North American installations using either SIA or Contact ID reporting formats (see section 8.5), enter *70 before the phone number to disable call-waiting.

15.6 CALL WINLOAD

Press and hold the **[0]** key, enter the **[INSTALLER CODE]** and press **[FORCE]** to dial the PC Telephone Number programmed in section **[560]** to communicate with WinLoad. The control panel and WinLoad will verify that the Panel Identifier and the PC Password match before establishing communication.

15.7 ANSWER WINLOAD

To perform on-site upload/downloading, connect your computer directly to the control panel using an ADP-1 line adapter. In WinLoad set *Dialing Condition* to *Blind Dial*. Program the panel telephone number in WinLoad and follow the ADP-1 Adapter's instructions. When the computer has dialed, press and hold the **[0]** key, enter the **[INSTALLER CODE]** and press **[ARM]** to manually answer WinLoad from the panel. Press **[DISARM]** to hang up.

15.8 EVENT BUFFER TRANSMISSION

SECTION [522]: OPTION [2]

If the Event Buffer contains 974 events since the last upload, the control panel will make two attempts to establish communication with a computer using WinLoad by calling the PC Telephone Number programmed in section **[560]**. WinLoad must be in *Wait To Dial* mode. When the system establishes communication, it will upload the contents of the Event Buffer to WinLoad. If communication is interrupted before completing transmission or if after two attempts, communication is not established, the system will wait until the Event Buffer attains another 974 events before attempting to re-communicate with the central station. When the Event Buffer is full, each subsequent new event will erase the oldest event in the buffer. The Event Buffer can hold 1024 Events.

15.9 CALL BACK FEATURE

SECTION [522]: OPTION [1]

For additional security, when a computer using WinLoad attempts to communicate with the control panel, the control panel can hang up and call the computer back to re-verify identification codes and re-establish communication. When the control panel hangs up, WinLoad automatically goes into *Wait For Call Mode*, ready to answer when the control panel calls back. Please note that the PC Telephone Number must be programmed in order to use the Call Back feature.

USER FEATURES

16.1 ARMING AND DISARMING FEATURES

Partitions can be armed using various arming methods:

16.1.1 Regular Arming

This method is used for the everyday arming of the system. All zones within the partition must be closed to arm the system. The system can also be Regular Armed by using a One-touch Feature (see section 6.8) or a keyswitch (see section 5.4.5). All users are able to Regular Arm the partition(s) assigned to their User Access Codes.

To Regular Arm, users:

- 1) Enter their **[ACCESS CODE]**
- 2) Press the **[ARM]** key. If the users have access to more than one partition, they can press the key corresponding to the desired partition or press **[0]** to arm all their assigned partitions.

16.1.2 Stay Arming

Stay Arming will partially arm the partition to permit the user to remain in the protected area. The programmed *Stay Zones* (see section 4.4.3) will not arm when Stay Arming a partition. For example, the doors and windows can be armed without arming the motion detectors. The system can also be Stay Armed by using a One-touch Feature (see section 6.8) or a keyswitch (see section 5.4.2). Only User Access Codes with the *Stay and Instant Arm* option enabled can Stay Arm a partition.

To Stay Arm, users:

- 1) Enter their **[ACCESS CODE]**
- 2) Press the **[STAY]** key. If the users have access to more than one partition, they can press the key corresponding to the desired partition or press **[0]** to arm all their assigned partitions.

16.1.3 Stay Arming with Delay

Stay Arming with Delay functions like Stay Arming except armed zones can be programmed with an *Entry Delay Timer* (see section 4.2.9). If these zones are accidentally triggered, the timer will start to allow the user time to disarm the partition(s).

16.1.4 Instant Arming

This feature is similar to *Stay Arming*. Instant Arming will partially arm the partition to permit the user to remain in the protected area, but all zones, including the entry/exit point, are changed to instant alarm zones. Therefore, if any armed zone is breached, the alarm will instantly be triggered. The system can also be Instant Armed by using a One-touch Feature (see section 6.8) or a keyswitch (see section 5.4.4). Only User Access Codes with the *Stay and Instant Arm* option enabled can Instant Arm a partition.

To Instant Arm, users:

- 1) Enter their **[ACCESS CODE]**
- 2) Press the **[5]** key. If the users have access to more than one partition, they can press the key corresponding to the desired partition or press **[0]** to arm all their assigned partitions.

16.1.5 Instant Arming with Delay

Instant Arming with Delay functions like Instant Arming except armed zones can be programmed with an *Entry Delay Timer* (see section 4.2.9). If these zones are accidentally triggered, the timer will start to allow the user enough time to disarm the partition(s).

16.1.6 Force Arming

Force Arming allows the user to arm a partition when Force zones are open (see section 4.4.4). Once the open zone in an armed partition is closed, however, the system will then arm it as well. This feature is commonly used when a motion detector is protecting an area that is occupied by a keypad. For example, during Force arming the motion detector will remain unarmed until the user exits the area that it protects. The system will then arm the motion detector. The system can also be Force Armed by using a One-touch Feature (see section 6.8) or a keyswitch (see section 5.4.3). Only User Access Codes with the *Force Arm* option enabled can Force Arm a partition.

To Force Arm, users:

- 1) Enter their **[ACCESS CODE]**
- 2) Press the **[FORCE]** key. If the users have access to more than one partition, they can press the key corresponding to the desired partition or press **[0]** to arm all their assigned partitions.

16.1.7 Disarming

Users can only disarm the partitions assigned to their User Access Codes. User Access Codes with the *Arm Only* option (see section 13.5.4) enabled cannot disarm.

To disarm, users:

- 1) Enter through a designated entry. The Entry Delay Timer will begin.
- 2) Enter their **[ACCESS CODE]**
- 3) Press the **[DISARM]** key

16.2 BYPASS PROGRAMMING

Bypass Programming allows users to program the alarm system to ignore specified zones the next time the system is armed. For a user to bypass a zone, the zone must have the Bypass option enabled, the User Access Code must have the Bypass option enabled, and the zone must be within the User Access Code's partition assignment.

To Bypass, users:

- 1) Enter their **[ACCESS CODE]**
- 2) Press the **[BYP]** key
- 3) Enter the zones' 2-digit number
- 4) Press **[ENTER]** key to exit

Users can also activate *Bypass Recall*. Bypass Recall reinstates all the zones that were bypassed the last time the partition(s) assigned to the User Access Code were armed.

To activate **Bypass Recall**, users:

- 1) Enter their **[ACCESS CODE]**
- 2) Press the **[BYP]** key
- 3) Press the **[MEM]** key
- 4) Press **[ENTER]** key to exit

16.3 CHIME ZONES

The keypads can be programmed to emit rapid, intermittent beeps whenever designated zones within their assigned partitions are opened or when they are opened within a certain time period. These zones are Chime Zones.

To program a **Chime Zone**, users:

- 1) Enter their **[ACCESS CODE]**
- 2) Press the **[9]** key
- 3) Press the **[1]** key
- 4) Enter the zones' 2-digit number
- 5) Press **[ENTER]** key to save

To program a **time period** when the Chime Zones are activated, users:

- 1) Enter their **[ACCESS CODE]**
- 2) Press the **[9]** key
- 3) Press the **[2]** key
- 4) Enter the time that keypads will **start** beeping when Chime Zones are opened according to the 24-hour clock (i.e. 9AM is 09:00 and 9PM is 21:00).
- 5) Enter the time that keypads will **stop** beeping when Chime Zones are opened according to the 24-hour clock (i.e. 9AM is 09:00 and 9PM is 21:00).
- 6) Press **[ENTER]** key to save

16.4 ACCESS CODES

Refer users to the appropriate User's Manual: LCD Keypad's User Manual or LED Keypads' User Manual.

16.5 NORMAL AND CONFIDENTIAL MODES

For LCD Keypads:

When no actions are being performed on the keypad, the keypad will remain in Normal Mode as shown in Figure 16-1 and will automatically display:

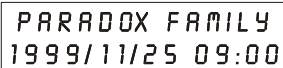
- The current status of the zones for every area the keypad is assigned
- The *Alarm Memory Display* if any alarms have occurred
- The *Trouble Display* if any troubles are occurring
- The current state of the *Indicator Lights*

In Confidential Mode:

- The zones and status messages will NOT be displayed
- The *Indicator Lights* will not illuminate

Depending on how the keypad was programmed, the user must press a key or enter a User Access Code to illuminate the *Indicator Lights* and activate *Normal Mode*.

Figure 16-1: Normal and Confidential Mode



PARADOX FAMILY
1999/11/25 09:00

In *Normal Mode*, the LCD screen displays "Paradox Family" and the time & date, as well as scroll the system, zone and trouble status for every area assigned to the keypad.



CONFIDENTIAL
1999/11/25 09:00

In *Confidential Mode*, the LCD screen only displays "Confidential" and the time & date. Depending on how your keypad is programmed, *Normal Mode* only appears once a button is pressed or a *User Access Code* is entered.

16.5.1 Scroll Restart

In Normal mode the keypad will scroll through the status of the different parts of your system. Press the **[CLEAR]** key at any time during Normal Mode to return to the beginning of the sequence and view the status of the areas assigned to the keypad.

For LED Keypads:

When no actions are being performed on the keypad, the keypad remains in Normal Mode and the LED keypad will illuminate:

- The AC Light if power is present
 - The Numerical Symbols representing any open zones
 - The Area Symbols if any areas are armed
 - The **[MEM]** Symbol if any alarms have occurred
 - The **[TRBL]** Symbol if any troubles are occurring
 - The **[BYP]** Symbol if zones are bypassed
- and shows the status of the STATUS LED.

In Confidential Mode all the LEDs are extinguished. Depending on how the keypad was programmed, the user must press a key or enter a *User Access Code* to illuminate the LEDs and activate *Normal Mode*.

16.6 KEYPAD SETTINGS

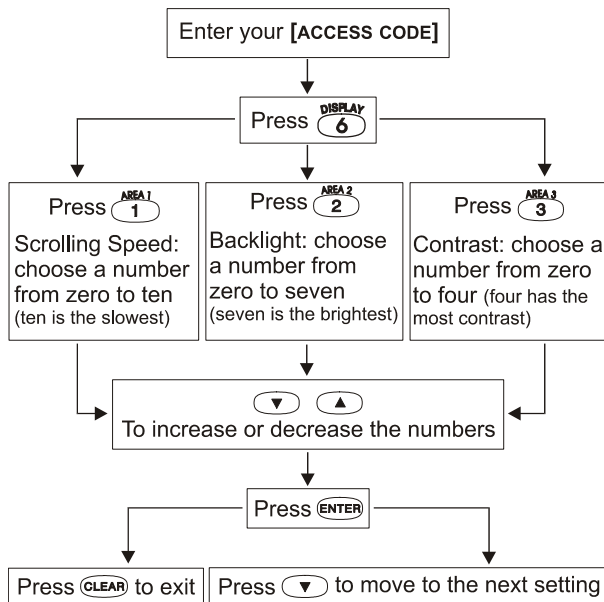
The keypad's setting can be modified to suit the user's needs.

For LCD Keypads:

- 1) **Scrolling Speed:** how long the messages will stay on the LCD screen before moving to the next message.
- 2) **Contrast:** how dark or pale characters will appear on the LCD screen
- 3) **Backlight:** the illumination behind the keys and the screen

Use the System Master Code to modify the settings as shown in Figure 16-2 on page 49.

Figure 16-2: LCD Keypad Settings



For LED Keypads:

Modify Backlight only:

- 1) Enter **[ACCESS CODE]**
- 2) Press the **[6]** key
- 3) Use the **[▲]** and **[▼]** keys to increase or decrease the illumination. The range is between zero and seven with seven as the brightest. ([10] LED = zero)

16.7 TROUBLE DISPLAY

When the system experiences problems or is tampered with, the Trouble Display will activate. In the LED Keypads, the **[TRBL]** Symbol illuminates. In the LCD Keypads, the Trouble Display will appear on the LCD screen. Keypads will only display troubles that occur in their assigned area(s).

Potential troubles have been sorted into eight groups. The Group headings are listed below with a brief explanation of the potential troubles sorted within each group.

TO VIEW THE TROUBLE DISPLAY:

- 1) Press the **[TRBL]** key
- 2) **For LEDs:** Press the Numerical Symbol corresponding to the Group heading to view the specific trouble.
For LCDs: Press the number representing the trouble and use the **[▲]** and **[▼]** keys to view the specific trouble.

GROUP [1]: SYSTEM

Trouble [1]: AC Failure

The control panel has detected a power failure. This means that the system is running on the backup battery.

Trouble [2]: Battery Trouble

The backup battery is disconnected, needs to be recharged, or replaced.

Trouble [3]: AUX Current Limit

Devices connected to the control panel have exceeded current limits (1.1A). The Auxiliary Output will shutdown until the trouble has been rectified.

Trouble [4]: Bell Current Limit

The bell or siren connected to the control panel has exceeded current limits (3A). The Bell/Siren Output will shutdown until the trouble is rectified.

Trouble [5]: Bell Absent

The control panel has detected that the bell or siren is not connected. When the bell output is not used, connect a 1kΩ resistor across the bell output or this trouble will re-occur.

Trouble [6]: ROM Check Error

The control panel registers a memory error. Contact your distributor for replacement.

GROUP [2]: COMMUNICATOR

Trouble [1]: TLM (Telephone Line Monitor)

The control panel is unable to access the telephone line.

Troubles [2] to [5]:

- [2] Fail to Communicate 1
- [3] Fail to Communicate 2
- [4] Fail to Communicate 3
- [5] Fail to Communicate 4

The control panel has tried all assigned telephone numbers and has failed to communicate with the Security Company.

Trouble [6]: Fail to Communicate PC

The control panel is unable to communicate with the WinLoad software.

GROUP [3]: MODULE TROUBLES

Trouble [1]: Module Tamper

The control panel registers that someone has triggered the tamper switch on a module.

Trouble [2]: ROM Check Error

The control panel registers a memory error in a module. Contact your distributor for replacement.

Trouble [3]: TLM Trouble

A module is unable to access the telephone line.

Trouble [4]: Fail to Communicate

A module has failed to communicate with the Security Company.

Trouble [5]: Printer Trouble

The control panel registers a problem with the printer connected to the Printer Module. Check printer for problems (paper jam, no paper, no power, etc.).

Trouble [6]: AC Failure

Module power failure.

Trouble [7]: Battery Failure

Module's battery is disconnected, needs to be recharged, or replaced.

Trouble [8]: Supply Output

Module has exceeded current limits.

GROUP [4]: NETWORK TROUBLES

Trouble [1]: Missing Keypad

A keypad is no longer communicating with the control panel.

Trouble [2]: Missing Module

A device is no longer communicating with the control panel.

Trouble [6]: General Failure

No communication between the devices and the control panel.

Trouble [7]: Network Overload

Too many devices (over 95) are connected on the network.

Trouble [8]: Network Communication Error

The network is having difficulty communicating between the devices and the control panel.

GROUP [5]: ZONE TAMPER

The zone or zones that have been tampered with will be displayed.

GROUP [6]: ZONE LOW BATTERY

If a wireless device's battery needs to be replaced, the zone that it is assigned to will be displayed. Also, the yellow light on the device will flash when this trouble is occurring.

GROUP [7]: ZONE FAULT

A smoke detector is experiencing a wiring problem, needs to be cleaned, or a wireless device is no longer communicating with its receiver (supervision loss).

GROUP [8]: CLOCK LOSS

The time and date have been reset to the default. To set:

- 1) Press the **[8]** key
- 2) Enter the hour and minutes according to the 24-hour clock (i.e. 9AM is 09:00 and 9PM is 21:00).
- 3) Enter the correct date according to yyyy/mm/dd.
- 4) Press **[CLEAR]** to exit.



If the Access Control feature is enabled in the system and the option *Door Access during Clock Loss* is ON (section [537] option [8]), only the System Master Code and User Codes with the Master feature enabled will be able to program the clock. Enter the System Master or a Master Code, press **[TRBL]**, then continue with the steps above.

16.8 EVENT RECORD DISPLAY

The Event Record Display can only be viewed through an LCD Keypad. The Event Record Display will record the user-initiated actions that occurred in the system as well as any alarms or troubles.

For example, when a valid code is entered, the User Access Code and the action taken (arm, disarm, etc.) is recorded.



Access Control events can only be viewed through an Access Control LCD Keypad (DGP2-641AC)

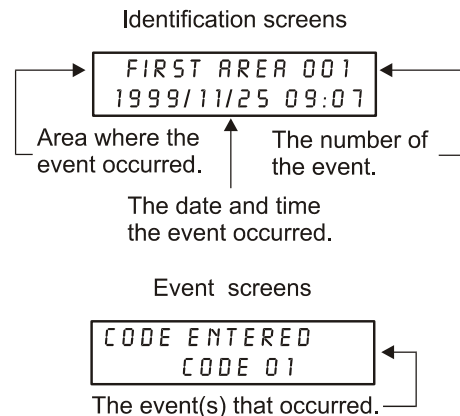
You have the choice of viewing the events in all the partitions at once or by individual area. In either case the most recent event is displayed first (see *Figure 16-3: Event Record screens*).

To view the events:

- 1) Enter the **[SYSTEM MASTER CODE]**
- 2) Press the **[7]** key
- 3) Press the **[0]** key for all partitions
Press the **[1]** key for Partition 1
Press the **[2]** key for Partition 2
Press the **[3]** key for Partition 3
Press the **[4]** key for Partition 4
- 4) Use the **[▼]** key to view subsequent events
- 5) Press the **[CLEAR]** key to exit

Once you have entered the Event Record Display, you can change the order that the Event Record screens (see *Figure 16-3: Event Record screens*) appear by pressing the **[7]** key. If you already know the number of the event you want to view, press the **[MEM]** key and then enter the event's number.

Figure 16-3: Event Record screens



INDEX

Sections

001 to 048	15	500	23, 37
049 to 056	18	501	20, 23, 24
101 to 148	15	502	23, 32, 33, 38
149 to 156	18	503	20, 33, 37, 39
200	17	504	17, 22, 39, 40, 42
201 to 216	17	505	20–21
217	16	506	24, 29
218	39	507	22
219	29	508	21
220	21	509	20–21
221	21	510	24, 29
222 to 225	21	511	22
226 to 229	21	512	21
230 to 233	15	513	20–21
234 to 237	23	514	24, 29
238 to 241	22	515	22
242 to 245	23	516	21
246 to 249	23	517	20–21
250 to 254	33	518	24, 29
255	31	519	22
256	17	520	21
257	29	521	26, 31
258	29	522	29, 31, 38, 46
259	29	522 to 536	29
260	29	537	43, 44, 45
261	29	550	28
270	29	551 to 554	28
271 to 274	20	555	46
301 to 332	43	556	46
340	43	560	46
341 to 355	44	561 to 564	28
361 to 375	44	600 to 625	26
381 to 392	44	626	20, 26
400	32	627	26
401	33	628 to 653	26
402	32	654	26
403	33	655 to 666	26
404	32	667 to 678	26
405	33	679 to 680	26
406	32	681 to 692	27
407	33	693 to 704	27
408	32	705	21, 27
409	33	706 to 711	27
450	37	712	29
451	46	712 to 716	27
452	46	717	28
		718	28

790 to 795	30
800	40
801	40
802 to 896	40–42
900	38
950	40
951	38
952	38
953	12, 38
954	38
955	38
961	13
962	13
965	13
966	13
970	37
975	37
976	37
977	37
978	37
979	37
990	37

A

AC Power	5
Access Alarm	43
Access Card	43
Access Card Assignment	42
Access Control feature	41
Access Control Terms	43
Access Level	44
Access Level Assignment	41
Account Codes	28
Activate Card	42
Ademco Contact ID	28
Ademco Express	28
Advanced Technology Zoning (ATZ)	17
Alarm	
On Forced Door	45
Alarm Transmission Delay. See Delay Alarm Transmission	
Alarm Types	17
Alternate Backup Option	29
AND Door Access Mode	44
Answer WinLoad	37
Arm Only	41
Armed Access Doors	42
Arming methods	47
Arming with Access Card	42
Skip Exit Delay	45
Assigning keyswitches to partitions	19
ATZ	17

Audible Alarm	
Bell Cut-off Timer	23
Pulsed	17
Steady	17
Tamper Recognition	24
Wireless Transmitter Supervision	23
Auto Zone Shutdown	16
Auto-Arming	
No Movement	20
No Movement Timer	21
Timed	20
Timer	20
Automatic Event Buffer Transmission	46
Auxiliary Power	5
Auxiliary Output	5
Calculating power consumption	7
Power Limitations	7
Power Supply Connections	8
Troubles	49
Away Arming. See Force Arming	
Away Zones. See Force Zones	

B

Backlight	48
Battery	5
Battery Test	5
Bell	
Bell terminals	5
Bell/siren Output	5
Bell/Siren Output During Fire Alarm	16
Sirens	5
Troubles	49
Broadcast	38
Burglar Alarm On Forced Door	45
Burglary Zones	15
Buzzer Zones	15
Bypass Programming	47
Bypass Recall	48
Bypass Zones	16

C

Call Direction	29
Call WinLoad	37
Cancel Communication	37
Chime Zones	48
CleanMeTM	10
Clock Loss	
Access during Clock Loss	45
Codes	
Alarm Report Codes	26
Arming Report Codes	26
Disarming Report Codes	26
Special Alarm Report Codes	26
Special Arming Report Codes	26
Special Disarming Report Codes	26
Special Tamper Report Codes	27
System Trouble Codes	27
System Trouble Restore Codes	27

Zone Restore Report Codes	26
Zone Tamper Report Codes	27
Zone Tamper Restore Codes	27
Connections	
Advanced Technology Zone (ATZ)	17
Bell/siren Output	5
DGP2-ZX4	11
Double Zone Connections	10, 17
in Noisy Environments	9
Keypad Zone Connections	10
Keyswitch Connections	10
Network Connections	9
PGM	9
Power	5
Single Zone Connections	9
Telephone Line Connections	5
Contrast	48
Control Panel Programming Mode	12
Current setting for charging battery	37

D

Daylight Savings Time	38
Delay Alarm Transmission	17
Delay Alarm Transmission Timer	17
Delay Between Dialing Attempts	29
Delayed 24Hr Fire Zone	15
DGP2-ZX4	11
Dialer	31
Digiplex Memory Key. See Paradox Memory Key	
Disabled	
Wireless Transmitter Supervision	23
Disarm with Access Card	42
Door Access Mode	43
Door Forced Open Restore event	45
Door Left Open	43
Door Left Open Restore event	44
Doors	
Access During Clock Loss	45
Assigning The Keypad To A Door	43
Burglar Alarm On Forced Door	45
Double Zone Connections	10
Duress	41

E

Earth Ground	5
Enable Reporting	26
Entry Delay Timers	15
Entry Delay zones	15
EOL Zones	17
ESL CleanMeTM Installation	10
Event Buffer	
Log Door Forced Open Restore In Event Buffer	44
Log Door Left Open Restore In Event Buffer	44
Log Request For Exit In Event Buffer	44
Event Record Display	50
Everyday arming. See Regular Arming	

Exit Delay	21
Exit Delay cancelled on Remote Arm	21
Exit Delay Termination	21
Extended Unlocked Period	42

F

Feature Select Programming	12
Fire Circuits	10
Fire Zone	10
Fire Zone, Delayed 24hr.	15
Fire Zone, Standard 24hr.	16
Follow zone	15
Force Arming	47
Force Zones	17
Forced Door	43
Function Keys, Installer	37

G

Ground	5
--------------	---

H

Hardware Reset	37
Holiday Programming	44
Hourly Test Transmission	29

I

Identifier code. See Panel Identifier	46
Input Numbers	
Keyswitch Numbering	18
Zone Numbering	15
Input Speed	17
Installer Code	40
Installer Function Keys	37
Installer Lock	37
Installer Test Mode	37
Instant Arming	47
Instant Arming with Delay	47
Instant zone	15
Intellizone	17

K

Keypad connections. See Connections	
Keypad Lockout	21
Keypad Zone Connections	10
Keyswitch	
Arm/Disarm	19
Connections	10
Definitions	18, 19
Disabled	19
Keyswitch Numbering	18
Maintained	19
Momentary	19
Options	18, 19
Partition Assignment	18, 19

L

LCD Display	
Confidential Mode	48
Keypad Settings	48
Shabbat Feature	38
Locate Module	38
Location & Mounting	5
Logging Access Control Events	44

M

Master Feature	41
Maximum Dialing Attempts	29
Memory Key	13
Module Programming Mode	12
Module Scan	38
Multiple Action Feature	42

N

Network Connections	9
in Noisy Environments	9
Network Voltmeter	38
No Bell Cut-Off on Fire Alarm	23
No Exit Delay on Remote Arm	21

O

One-touch Features	21
OR Door Access Mode	44

P

Pager Reporting Format	29
Panel Answer Options	46
Panel Partition Assignment	37
Panel Programming Mode	12
Panic Options	24
Paradox Memory Key	13
Partitioning	37
PCB Layout	6
PGM	9
As a 2-wire smoke detector	10
As a 4-wire smoke detector	11
Connections	9
PGM Activation Event	32
PGM Deactivation Event	33
PGM Delay Timers	33
PGM Programming Table	34–36
PGM Time Base Selection	33
Relay	9
Power Supply Connections	8
Power Unit Consumption Table	7
Problems. See Trouble Display	
Programmable Outputs. See PGM	
Programming	12
Decimal Programming	12
Feature Select Method	12
Hexadecimal Programming	12

Level Programming	12
Modules	12, 38
Panel Programming Mode	12
Paradox Memory Key	13
Zone Programming	14

Pulse formats. See Standard Pulse Formats

Pulsed Audible Alarm	17
----------------------------	----

R

Record REX events	44
Record the Door Forced Open Restore events	45
Record the Door Left Open Restore events	44
Record. See Event Record Display	
Recycle Alarm	23
Recycle Delay	23
Regular Arming	47
Report Only	17
Reporting Formats	28
Request for Exit (REX) event	44
Reset	
Hardware	37
Module	38
Software	37
System Master Code Reset	40
Restrict Arming on	
Power Failure	20
Supervision Loss	20
Tamper	20
Ring-back	22

S

Schedule	44
Schedule Assignment	41
Scrolling Speed	48
Shabbat Feature	38
SIA FSK	28
Silent Alarm	17
Tamper Recognition	24
Silent Alarms	
Wireless Transmitter Supervision	23
Sirens	5
Skip Exit Delay When Arming With Card	45
Smoke Detector	10
CleanMeTM feature	10
Special Telephone Number Keys	28
Standard 24Hr Fire Zone	16
Standard Pulse Formats	28
Stay Arming	47
Stay Arming with Delay	47
Stay Delay zone	16
Stay Zones	16
Supervision Bypass Options	23
Swinger Shutdown. See Auto Zone Shutdown	
System Master Code Reset	40

T

Tamper	23
Tamper Bypass Options	24
Tamper Recognition	
Audible Alarm	24
Disabled	24
Silent Alarm	24
Trouble only	24
Telephone Line Connection	5
Test Report	37
TLM Fail Timer	31
Transformer	5
Trouble Display	49
Troubles	49

W

WinLoad	46
Answer WinLoad	37, 46
Call WinLoad	37, 46
Cancel Communication	37
Wireless Transmitter Supervision Options	23

Z

Zones	
24Hr Burglary zone	15
24Hr Buzzer	15
Alarm Transmission Delay	17
Bypass	16
Connections	9
Definition	14, 15
Delayed 24Hr Fire Zone	15
Disabled	15
Doubling	17
Entry Delay	15
EOL	17
Follow	15
Force Zone	17
Generates a report only	17
Input Speed	17
Instant	15
Intellizone	17
Options	14
Partition Assignment	14, 16
Pulsed Audible Alarm	17
Silent Alarm	17
Standard 24Hr Fire Zone	16
Stay Delay zone	16
Stay Zone	16
Steady Audible Alarm	17
Zone Doubling (ATZ)	17
Zone Numbering	14, 15
Zone Options	16
Zone Parameters	14

WARNINGS

FFC Warnings

IMPORTANT INFORMATION

This equipment complies with Part 68 of the FCC rules subpart D and CS-03. Inside the cover of this equipment is a label that contains, among other information, the FCC registration number of this equipment.

NOTIFICATION TO TELEPHONE COMPANY

Upon request, customer shall notify telephone company of particular line to which the connection will be made and provide the FCC registration number and the ringer equivalence of the protective circuit.

FCC REGISTRATION NUMBER: 5A7CAN-22633 - AL - E
RINGER EQUIVALENCE NUMBER: 0.1B (U.S. & CANADA)
USOC JACK: RJ31X (USA), CA31A (CANADA)

TELEPHONE CONNECTION REQUIREMENTS

Except for telephone company provided ringers, all connections to the telephone network shall be made through standard plugs and telephone company provided jacks, or equivalent, in such a manner as to allow for easy, immediate disconnection of terminal equipment. Standard jacks shall be so arranged that, if plug connected thereto is withdrawn, no interference to operation of equipment at customer's premises which remains connected to telephone network shall occur by reason of such withdrawal.

INCIDENCE OF HARM

Should terminal equipment/protective circuitry cause harm to telephone network, telephone company shall, where practicable, notify customer that temporary disconnection of service may be required; however, where prior notice is not practicable, the telephone company may temporarily discontinue service if action is deemed reasonable in circumstances. In case of temporary discontinuance, telephone company shall promptly notify customer and will be given opportunity to correct the situation.

CHANGES IN TELEPHONE COMPANY EQUIPMENT OR FACILITIES

The telephone company may make changes in its communication facilities, equipment operations or procedures, where such actions are reasonably required and proper in its business. Should any such changes render customer's terminal equipment incompatible with the telephone company facilities, the customer shall be given adequate notice to effect the modifications to maintain uninterrupted service.

GENERAL

This equipment shall not be used on coin telephone lines. Connection to party line service is subject to state tariffs.

RINGER EQUIVALENCE NUMBER (REN)

The REN is useful to determine the quantity of devices that you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, sum of the REN's of all devices connected to one line should not exceed five (5). To be certain of the number of devices that you may connect to your line, you may want to contact your local telephone company.

EQUIPMENT MAINTENANCE FACILITY

If you experience trouble with this telephone equipment, please contact facility indicated below for information on obtaining service or repairs. The telephone company may ask that you disconnect this equipment from network until problem is corrected or until you are sure that the equipment is not malfunctioning.

FCC PART 15, WARNINGS: INFORMATION TO USER

This equipment has been tested and found to comply with the limits for Class B digital devices, pursuant to Part 15 of 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 equipment intermittently, the user is encouraged to try to correct the interference by one or more of the following measures: (1) reorient or relocate the receiving antenna; (2) increase the separation between the equipment and receiver; (3) connect the equipment to an outlet on a circuit other than the one to which the receiver is connected, or (4) consult the dealer or an experienced radio/tv technician for assistance.

CAUTION:

Changes or modifications not expressly approved by PARADOX SECURITY SYSTEMS could void the user's authority to operate the equipment.

UL and ULC Warnings

UL AND C-UL INSTALLATION NOTES

This equipment is UL listed in accordance with standard UL1023 (Household Burglar -- Alarm Systems Units), standard UL985 (Household Fire Warning Units) and standard UL1635 (Digital Alarm Communicator System Units). This equipment has the capability of being programmed with features not verified for use in UL installations. To stay within these standards, the installer should use the following guidelines when configuring the system:

- All components of the system should be UL listed for the intended application.
- If the system will be used for "Fire" detection, the installer should refer to NFPA Standards #72, Chapter 2. In addition, once installation is complete, the local fire authority must be notified of the installation.
- This equipment must be verified by a qualified technician once every three years.
- All keypads must use a tamper switch.
- Maximum allowed entry delay is 45 seconds.
- Maximum allowed exit delay is 60 seconds.
- Minimum 4 minutes for bell cut-off time.
- The following features do not comply with UL requirements: Bypass Recall, Shabbat, Auto Trouble Shutdown, and "No AC Fail" display.
- Do not connect the primary indicating device to a relay. The installer must use the bell output.

All outputs are Class 2 or power-limited, except for the battery terminal. The Class 2 and power-limited fire alarm circuits shall be installed using CL3, CL3R, CL3P, or substitute cable permitted by the National Electrical Code, ANSI/NFPA 70.

CTR-21 Warnings

The equipment has been approved in accordance with Council Decision 98/482/EC for pan-European single terminal connection to the public switched telephone network (PSTN). However, due to differences between the individual PSTNs provided in different countries, the approval does not, of itself, give an unconditional assurance of successful operation on every PSTN network termination point. In the event of problems, you should contact your equipment supplier in the first instance.

WARRANTY

The Seller warrants its products to be free from defects in materials and workmanship under normal use for a period of one year. Except as specifically stated herein, all express or implied warranties whatsoever, statutory or otherwise, including without limitation, any implied warranty of merchantability and fitness for a particular purpose, are expressly excluded. Because Seller does not install or connect the products and because the products may be used in conjunction with products not manufactured by Seller, Seller cannot guarantee the performance of the security system. Seller obligation and liability under this warranty is expressly limited to repairing or replacing, at Seller's option, any product not meeting the specifications. In no event shall the Seller be liable to the buyer or any other person for any loss or damages whether direct or indirect or consequential or incidental, including without limitation, any damages for lost profits, stolen goods, or claims by any other party, caused by defective goods or otherwise arising from the improper, incorrect or otherwise faulty installation or use of the merchandise sold.

ATTACHMENT LIMITATION NOTICE

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

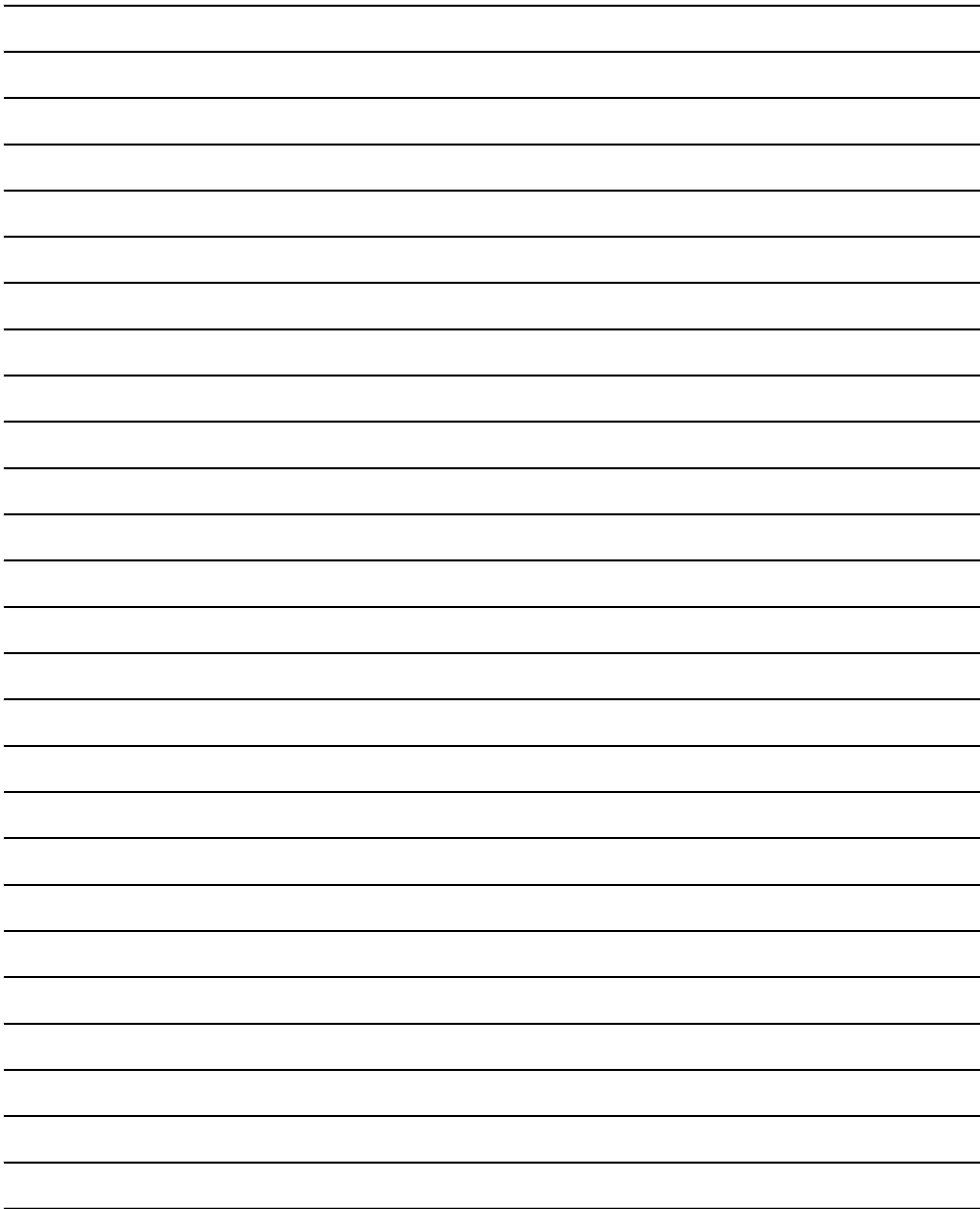
Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all of the devices does not exceed 100.

Industry Canada certification is only applicable to installation of devices which include transformers approved by the Canadian Standards Association (CSA).

[illegible]



P ▲ R ▲ D O X[®]
S E C U R I T Y S Y S T E M S

780 Industrial Blvd., St-Eustache, Montreal, Quebec, Canada J7R 5V3
Fax: (450) 491-2313 <http://www.paradox.ca>

PRINTED IN CANADA - 05/2002
DGPXEI-08