Honeywell

VISTA-128BPT/ VISTA-250BPT/ VISTA-128BPTSIA

Commercial Burglary Partitioned Security System With Scheduling

Installation and Setup Guide

800-06903V4 10/16 Rev B

Table of Contents

List of Figures

Section 1: How To Use The Manual

Before you begin using this manual, it is important that you understand the meaning of the following symbols (icons).

UL These notes include specific information that must be followed if you are installing this system for a UL Listed application.

These notes include information that you should be aware of before continuing with the installation, and that, if not observed, could result in operational difficulties.

This symbol indicates a critical note that could seriously affect the operation of the system, or could cause damage to the system. Please read each warning carefully. This symbol also denotes warnings about physical harm to the user.

ZONE PROG?
1 = YES 0 = NO 0

Many system options are programmed in an interactive mode by responding to alpha keypad display prompts. These prompts are shown in a single-line box.

***00** Additional system options are programmed via data fields, which are indicated by a "star" (*) followed by the data field number.

Product Model Numbers

Unless noted otherwise, references to specific model numbers represent Honeywell products.

SIA CP-01 Quick Reference Chart

The minimum required system for SIA CP-01 is a VISTA-128BPTSIA Control, one of the following keypad models; 6160, TUXS, TUXW, 6280S, or 6280W and a UL Listed Bell.

Item	Feature	Range	Shipping Default	SIA Requirement*
*09	Entry Delay # 1	02 – 15multiplied by 15 seconds 00 = 240 sec (4 minutes)	30 Seconds	At least 30 Seconds **
*10	Exit Delay #1	03 – 15 multiplied by 15 seconds	60 Seconds	60 Seconds
*11	Entry Delay # 2	02 – 15 multiplied by 15 seconds 00 = 240 sec (4 minutes)	30 Seconds	At least 30 Seconds **
*12	Exit Delay #2	03 – 15 multiplied by 15 seconds	60 Seconds	60 Seconds
*28	Power Up in Previous State	0 = no 1 = yes	Yes	Yes
*57	Dynamic Signaling Priority	0 = Primary dialer 1 =Communicator as first reporting destination	0 (primary dialer)	0 (primary dialer)
*84	Swinger Suppression	01-06 = 1–6 alarms	1 alarms	1 alarm
*88	Abort Window Time (for non-fire zones)	1 = 15 seconds 2 = 30 seconds 3 = 45 seconds	30 Seconds	At least 15 Seconds **
1*21	Exit Time Reset	0 = no 1 = Resets Exit Delay to programmed value after zone is closed and then faulted prior to end of exit delay.	1 (Enabled)	1 (Enabled)
1*22 – 1*25	Cross Zoning	Zone 001 – 250 000, 000 = Disabled	Disabled	Enabled and two (or more) zones programmed
1*42	Call Waiting Defeat	0 = no 1 = yes	Disabled (0)	Enabled if user has call waiting
1*61	Abort Verify	0 = Disable 1 = Enable	Enabled	Enabled
Zone Programming Auto Stay Zone, Zone type 04 has this feature enabled by default	Auto Stay Arm or Occupied Premises	0 = Disable 1 = Enable	1 (Enabled)	Enabled

Item	Feature	Range	Shipping Default	SIA Requirement*
Zone Programming (Abort Window Enable)	Abort Window (for non-fire zones)	0 = no abort window 1 = yes, use abort window according to ∗88 selection	1 = yes	Yes (all non-fire zones)
Zone Programming (Swinger Suppression Enable)	Swinger Suppression Enable	0 = no suppression 1 = yes, suppress alarms according to ∗84 selection	Yes (enabled)	Yes (enabled (all zones))
Zone Programming Tamper Option	Fire Alarm Verification	For Zone Response Type 16 (Fire) tamper selection must be set to "0"	Disabled	Enabled unless sensors can self-verify
-	Exit Time and Progress Annunciation/Disable for Remote Arm (Not Evaluated for SIA CP-01)	Always Enabled	Enabled	Enabled
-	Programmable Cross Zoning Time	Both zones must be faulted within 5 minutes	Per Manufacturer	Per walk path in protected premises
-	Cancel Window	5 minutes	Enabled	Not required to be programmable
-	Cancel Annunciation - Keypad displays "Alarm Cancel" when report is received	NA	Enabled	Enabled
User Authority Level 6	Duress Feature	NA	Disabled	Disabled

* Programming at installation may be subordinate to other UL requirements for the intended application.
** Combined Entry Delay and Abort Window should not exceed 1 minute.

NOTES:

- Using the Call Waiting Cancel feature on a non-Call Waiting line will prevent successful communication to the central station.
- The control unit must be installed with a local sounding device and an off-premise transmission for Contact ID communication format.
- Refer to the ***User Guide*** for procedures on Testing the System.
- During Test mode, no alarm reports are sent to the central monitoring station.

Section 2: General Description

About the VISTA-128BPT/VISTA-250BPT

All references to the VISTA-128BPT also pertain to the VISTA-128BPTSIA. The differences between the two panels are outlined in the SIA CP-01 Quick Reference Chart located at the beginning of this manual.

The VISTA-128BPT/VISTA-250BPT is an 8-partition, UL Listed control panel with the following features:

- Supports hardwired, polling loop, and wireless zones
- Supervision of bells, keypads, RF receivers, and output devices
- Scheduling capabilities (allows certain operations to be automated)
- The VISTA-128BPT/VISTA-250BPT can interface with the following devices:
- Up to six 6280 Graphic/Touch-Screen keypads
- AlarmNet Total Connect (Remote Interactive Service) allows access from a wireless smart phone or web browser via any Total Connect 2 compatible AlarmNet device.
- Voice Keypad (6160V)

UL Voice Keypad 6160V cannot be used for SIA Installations.

- An ecp Communication Device that can send Contact ID messages
- An access control system by using the ADEMCO VistaKey module (via the polling loop)

UL The access control function is not Listed for use with the VISTA-128BPT/VISTA-250BPT Control Panel in a UL installation.

NOTE:All references in this manual for number of zones, number of user codes, number of access cards, and the event log capacity, use the VISTA-250BPT's features. The following table lists the differences between the VISTA-128BPT and the VISTA-250BPT control panels. All other features are identical.

Feature	VISTA-128BPT	VISTA-250BPT
Number of Zones	128	250
Number of User Codes	150	250
Number of Access Cards	250	500
Event Log Capacity	512	1000
VistaKey Modules	8	15

Features

Hardwire and Optional Expansion Zones

- Provides **nine hardwire zones**.
- Supports up to **16 2-wire smoke** detectors on zone 1.
- Automatic **4-wire smoke detector reset** using the J7 output when a code + off is entered.
- Triggers the built-in sounders on other hardwired smoke detectors if one smoke detector annunciates an alarm.
  NOTE: This feature requires a 4204 Relay Module.
- Provides **tamper supervision** on the hardwire zones.
- Supports up to 241 **additional hardwired expansion zones** (119 for the VISTA-128BPT) using a built-in polling (multiplex) loop.
- Supports up to 249 **wireless expansion zones** (127 for the VISTA-128BPT) (fewer if using hardwire and/or polling loop zones).

UL The 5881ENHC RF Receiver, 5869 Holdup Switch Transmitter and 5817CB Wireless Commercial Household Transmitter are listed for UL Commercial Burglary applications. All other RF receivers and transmitters are not listed for UL Commercial Burglary applications.

ULC Wireless devices are not ULC Listed and cannot be used for ULC Installations.

- Can program burglary zones as silent in the alarm condition (alarm output is silent and the keypad does not display or sound the alarm).
- Provides **three keypad panic** keys: 1 + * (A), * + # (B), and 3 + # (C).

UL Use of Remote Interactive Service (Total Connect) is not permitted in UL installations.

NOTE: If using Total Connect Remote Interactive Services, the virtual keypad must be assigned to a burglary partition, and the GOTO feature (program field 2*18) must be "0" (disabled) for partition 1 (the fire partition) so that the Fire system cannot be accessed remotely. This is the system default setting.

- **Anti-Mask** is used if an interior zone types 04 (interior) or 10 (interior with delay) and input type 06 (serial poll) are selected. The trouble report code is used to report the masking.
- A **Smart contact** option that may be selected for devices that support this feature such as the 5193SDT Smoke Detector or PIRs.
- **Battery sensing hardware** that can sense when the battery voltage is too low and prevents deep discharging from not occurring.

Peripheral Devices

- Supports up to **31 addressable devices**, (keypads, RF receivers, relay modules, etc.).
- **Supervises devices** (keypads, RF receivers, and relay modules) and individual relays (up to 32), as well as system zones (RF receivers and keypad panics).
- Provides **96 outputs** using 4204 Relay Modules and V-PLEX Relay Modules that can activate outputs in response to system events (alarm condition), at a specific time of day, at random times, and manually using the #70 Relay Command Mode.
- Supports a **Momentary Keyswitch** on any one of the system's eight partitions, using zone seven (Event/Actions).

Arming/Disarming and Bypassing

- Can arm the system with zones faulted **(Vent Zone)**. These zones are automatically bypassed and can be programmed to automatically unbypass when the zone restores.
- Can arm with entry/exit and interior type zones faulted **(Arm w/Fault)**. These zones must be restored before the exit delay expires, otherwise an alarm is generated.

UL

- Vent zones cannot be used in UL installations.
- You **must disable** the Force Arm option (used in conjunction with the Arm w/Fault option), in UL installations.

ULC

You **must disable** the Force Arm option (used in conjunction with the Arm w/Fault option), in ULC Installations.

- Provides **global arming** capability (ability to arm all partitions the user code has access to in one command).
- Can **Quick Exit** an armed premises without having to disarm and then rearm the system.

UL

Quick Exit is not permitted for use with the VISTA-128BPT/VISTA-250BPT Control Panel in a UL installation.

- Can be armed in one of **three STAY modes** or Instant modes, automatically bypassing specific burglary zones regardless of the zone response type.
- Can **automatically bypass specific zones** if no one exits the premises after arming (Auto-STAY). Auto-STAY will not occur if the system is armed via an RF transmitter, scheduling, access control, keyswitch, RS232 (TB4) automation or downloading.
- Can **bypass a group of zones** with one set of keystrokes.
- Supports **Exit Error Logic,** whereby the system can tell the difference between a regular alarm and an alarm caused by leaving an entry/exit door open. If the system is not subsequently disarmed, faulted E/E zone(s) and/or interior zones are bypassed and the system arms.
- Supports **Recent Close report**, which is designed to notify the central station that an alarm has occurred within 2 minutes after the exit delay has expired.

Partitioning

- Can **control eight separate areas independently**, each functioning as if it had its own separate control.
- Provides a **Common Lobby partition**, which can be programmed to arm automatically when the last partition is armed, and to disarm when the first partition is disarmed.
- Provides a **Master partition** (9), used for the purpose of viewing the status of all partitions at the same time.
- Can display fire, burglary, panic, and trouble conditions at all other partitions' keypads (selectable option)

Scheduling

ULC Scheduling cannot be used for ULC Installations.

- Can **automate system functions,** such as arming, disarming, and activation of outputs (e.g., lights).
- Provides **access schedules** (for limiting system access to users by time).
- Provides an **End User Output Programming** Mode, allowing the user to control outputs

Access Control

- Supports up to **15 VistaKey modules** (15 access points) (VISTA-128BPT supports 8 modules), which are used for access control. It is a single-door access control module.
- Support up to **500 access cards** (250 in VISTA-128BPT).
- Stores access control events in the event log.

System Communication

- Supports ADEMCO Contact ID; ADEMCO 10-Digit Contact ID and 4+2 Express formats.
- Supports **Dynamic Signaling** feature, which prevents redundant signals being sent to the central station when both the built-in dialer and Communication Devices are used.
- Provides the **Dialer Queue Report** in the event of a loss of communications between the dialer and the central station, i.e. telco loss. The total events that will be queued up are 128 (96 Burg + 32 Life Safety). A Dialer Queue Overflow report (E354) will be sent if the report queue goes beyond its limits.

  NOTE: Life Safety includes Fire, CO, 24 HR Silent/Audible/Auxiliary, and Duress. Life Safety events may go beyond 37 (up to 128) if there are no Burg events in the queue.

Downloading

- Supports upload and download capability.
- Downloadable via phone line or compatible AlarmNet communicator using Compass 2.0 revision 2.2.75 or above.
- Can download access control cardholder information

NOTE: Updates can be found on MyWebTech (https://mywebtech.honeywell.com/)

Event Log

- Provides an event log (history log) that can store up to 1000 events (512 for VISTA-128BPT).
- Can view the event log on an alpha or graphic/touch-screen keypad.

Telephone Line Fault Monitor

- This feature is enabled in field *30.
- The panel will indicate "PHONE LINE CUT" on the keypad when phone line voltage drops below 2VDC for approximately 120 seconds.
- The panel will send/log CID code E351 Telco Fault over an ECP Communicator. (Please note that the E351 report needs to be enabled in System Group 2, report code programming under "TELCO TROUBLE".)
- R351 Telco Fault is sent/logged when phone line voltage has returned for approximately 60 seconds.

V-PLEX® Smart Contact Technology

- **Automatic suppression of fault/restores when disarmed**
  a. Smart V-PLEX® sensors such as the DT7500SN, and IS2500SN polling loop motion detectors can be set to stop sending fault/restore signals while the partition is disarmed. This prevents the polling loop from slowing down due to high bus activity in busy areas.
  b. The feature is enabled by Zone in Zone Programming.
  c. When enabled, within about 5 minutes of program exit, the panel will send the command to the Smart Contacts to turn off their LED and stop sending faults/restores to the system. (The DT-7500SN and IS2500SN will turn off their LED unless the LED DIP switch is set to ON, in which case the LED will always remain enabled.)
- **Automatic Test Mode entry**
  a. Upon entering Code + 5 (Burglary Walk Test Mode), the panel will again tell the PIR to enable the LEDs and start sending faults/restores.
  b. The LED will remain enabled until the Burglary Walk Test mode is exited.
  c. Removing and replacing the cover of the DT7500SN and IS2500SN, or power-cycling these sensors will also put them in the walk test mode, enabling the LEDs and sending of faults/restores for 10 minutes.

  NOTE: Regardless of Smart Mode, Tamper and Supervision Failures are sent without delay.
- **PIR Anti-Mask**
  a. Capable motion detectors such as the DT7500SN have an "Anti-Mask" feature that will alert the panel when the lens has been blocked. (For DIP switch settings related to this feature, refer to the motion detector documentation.)
  b. Anti-Mask can be enabled in zone programming if a zone types 04 (interior) or 10 (interior with delay) and input type 06 (serial poll) are selected. In the event masking occurs, the message "PIR masked" will be displayed on the keypad, and a trouble report code is used to report the masking.
- **Smoke Detector Maintenance**
  Provides Maintenance Signal support for certain smoke detectors, such as the 5193SD and 5193SDT V-PLEX detectors, as well as the 5808W3.
- **Operation**
  When programmed as a "**Smart Contact**" in zone programming, a sensor which is capable of providing a high or low sensitivity condition (e.g., sensor is dirty) will trigger a message on the keypad, a dialer report, and an event log entry. The display message will indicate HSENSxxx or LSENSxxx, where xxx is the zone number.

Additional Features

- Provides up to **60 installer-defined, custom words** that can be used for zone descriptors.
- Provides **32 keypad macro commands** (each macro is a series of keypad commands of up to 32 keystrokes) using the A, B, C, and D keys by partition.
- Provides **cross-zone capability**, which helps prevent false alarms by preventing a zone from going into alarm unless its cross-zone is also faulted within a 5-minute period.
- Contains a **built-in User Manual**, which provides the end user with a brief explanation of the function of a key when the user presses any of the function keys on the keypad for 5 seconds.
- Provides an **RS232 input** (TB4) for serial data. This is useful for interfacing the system with Automation software. Automation software cannot be used if a serial printer is used on the system.

Section 3: Partitioning

Theory of Partitioning

This system provides the ability to arm and disarm up to eight different areas, as if each had its own control. These areas are called partitions.

A Partitioned system allows the user to disarm certain areas while leaving other areas armed, or to limit access to certain areas to specific individuals. Each system user can be assigned to operate any or all partitions, and can be given a different authority level in each.

Before anything can be assigned to those partitions, you must first determine how many partitions (1-8) are required and enable in programming. Following are some facts you need to know about partitioning.

Keypads

Each keypad must be given a unique "address" and be assigned to one partition. It can also be assigned to Partition 9 if Master keypad operation is desired. (See "Master Keypad Setup and Operation" later in this section.)

Zones

Each zone must be assigned to one partition. The zones assigned to a partition will be displayed on that partition's keypad(s) only.

Users

Each user may be given access to one or more partitions. If a user is to operate more than one partition and would like to arm/disarm all or some of those partitions with a single command, the user must be enabled for Global Arming for those partitions (when entering user codes).

A user with access to more than one partition (multiple access) can "log on" to one partition from another partition's keypad, provided that program field 2∗18: Enable GOTO is enabled for each partition he/she wants to log on to from another.

A partition can be selected as a "*common lobby*" partition, and other partitions can affect this partition by causing arming/disarming of this partition to be automated (see "Common Lobby Logic" later in this section).

Setting-Up a Partitioned System

The basic steps to setting up a partitioned system are described below. If you need more information on how to program the options, see *SECTION 4: Programming*.

1. Determine how many partitions the system will consist of (programmed in field 2*00).
2. Assign keypads to partitions (*Device Programming* in the *#93 Menu Mode*).
3. Assign zones to partitions (*Zone Programming* in the *#93 Menu Mode*).
4. Confirm zones are displayed at the keypad(s) assigned to those partitions.
5. Assign users to partitions.
6. Enable the GOTO feature (program field 2*18), which allows a user code with multiple-access the ability to log on to another partition. (Compatible with an alpha keypad only.)
7. Program partition-specific fields (see the Data Field Descriptions section).

Common Lobby Logic

When an installation consists of a partition shared by users of other partitions in a building, that shared partition may be assigned as the "common lobby" partition for the system (program field 1*17). An example of this might be in a medical building where there are two doctors' offices and a common entrance area (see example that follows explanation).

The Common Lobby feature employs logic for automatic arming and disarming of the common lobby. Two programming fields determine the way the common lobby will react relative to the status of other partitions. They are: 1*18 Affects Lobby and 1*19 Arms Lobby.

1∗18 Affects Lobby (must be programmed by partition)

Setting this field to 1 for a specific partition causes that partition to affect the operation of the common lobby as follows:

a. When the first partition that affects the lobby is disarmed, the lobby is automatically disarmed.
b. The common lobby cannot be armed unless every partition selected to affect the lobby is armed.

1∗19 Arms Lobby (must be programmed by partition)

Setting this field to 1 for a specific partition causes that partition to affect the operation of the common lobby as follows:

a. The common lobby cannot be armed unless every partition selected to affect the lobby is armed.

b. Arming a partition that is programmed to arm the lobby causes the system to automatically attempt to arm the lobby.

If any faults exist in the lobby partition, or if another partition that affects the lobby is disarmed, the lobby cannot be armed, and the message "UNABLE TO ARM LOBBY PARTITION" is displayed.

You cannot select a partition to "arm" the lobby unless it has first been selected to "affect" the lobby. Do not enable field 1∗19 without enabling field 1∗18.

The following chart sums up how the common lobby partition will operate.

1∗18 Affects Lobby	1∗19 Arms Lobby	Disarms when partition disarms?	Attempts to arm when partition arms?	Can be armed if other partitions disarmed?
0	0	NO	NO	YES
1	0	YES	NO	NO
1	1	YES	YES	NO
0	1	---ENTRY NOT ALLOWED---		

Example

Here is an example of how the lobby would react in a typical setup.

User #1 has access to Office #1 and the Common Lobby.

User #2 has access to Office #2 and the Common Lobby.

Office #1 is set up to affect the Common Lobby, but not arm it.

Office #2 is set up to affect and arm the Common Lobby.

NOTE: In the tables below, the notations in parentheses ( ) indicate the current status of the other partition when the user takes action.

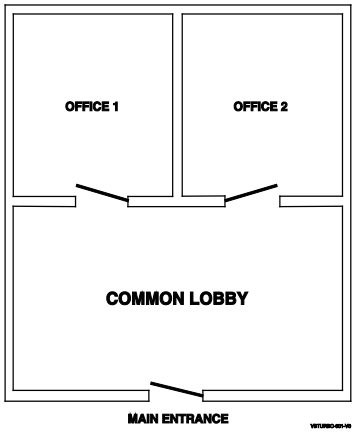


Figure 1: Common Lobby

Sequence #1:

User #	Office 1	Office 2	Lobby Action
1	Disarms	(Armed)	Disarms
2	(Disarmed)	Disarms	No Change
1	Arms	(Disarmed)	No change
2	(Armed)	Arms	Arms

Sequence #2:

User #	Office 1	Office 2	Lobby Action
2	(Armed)	Disarms	Disarms
1	Disarms	(Disarmed)	(No change)
2	(Disarmed)	Arms	No Change
1	Arms	(Armed)	No Change

Notice that in sequence #1, because Office #2 was the last to arm, the lobby also armed (Office #2 is programmed to affect and arm the lobby). In sequence #2, the lobby could not arm when Office #2 armed, because Office #1, which affects the lobby, was still disarmed.

When Office #1 armed, the lobby still did not arm because Office #1 was not programmed to arm the lobby. User #1 would have to arm the lobby manually. Therefore, you would want to program a partition to affect and arm the lobby if the users of that partition are expected to be the last to leave the building.

How User Access Codes Affect the Common Lobby

Codes with Global Arming

- If a code is given "G*lobal Arming*" when it is defined (see SECTION 9: User Access Codes), the keypad prompts the user to select the partitions they want to arm.
- Only the partitions the user has access to be displayed. This allows the user to choose the partitions to be armed or disarmed, and so eliminates the "automatic" operation of the lobby. Keep in mind, however, that if a user attempts to arm all, and another "*affecting*" partition is disarmed, the user cannot arm the lobby, and the message "UNABLE TO ARM LOBBY PARTITION" is displayed.

Codes with Non-Global Arming

If a user arms with a non-global code, the lobby partition operation is automatic, as described by fields 1*18 and 1*19.

Other Methods of Arming/Disarming

Common Lobby logic remains active when arming or disarming a partition that affects and/or arms the common lobby in one of the following manners:

- Quick-Arm
- Keyswitch
- Wireless Button
- Wireless Keypad

NOTE: Common Lobby Logic is NOT active when Disarming using a Vista-Key card grant.

Arming/Disarming Remotely

If a user arms or disarms remotely (through Compass downloading software or AlarmNet® Total Connect Remote Services), the lobby does not automatically follow another partition that is programmed to arm or disarm the lobby. The lobby must be armed separately, after arming all affecting partitions first.

Auto-Arming/Disarming

If scheduling is used to automatically arm and/or disarm partitions, the common lobby partition does not automatically follow another partition that is programmed to arm or disarm the lobby.

The lobby must be included as a partition to be armed/disarmed and must be scheduled as the last partition armed.

If you are using auto-arming, make sure that the **Auto-Arm Delay** and **Auto-Arm Warning** periods, for the lobby partition, (fields 2*05 and 2*06) combined are longer than that of any other partition that affects the lobby. This causes the lobby to arm last.

Master Keypad Setup and Operation

Although this system has eight actual partitions, it provides an extra partition strictly for the purpose of assigning keypads as **Master keypads** for the system.

- Assigning any keypad to Partition 9 (in *Device Programming* in the *#93 Menu Mode)* identifies that keypad a Master keypad.
- A Master keypad reflects the status of the entire system (Partitions 1-8) on its display at one time.
- This eliminates the need for a building security officer to have to log on to various partitions from one partition's keypad to find out where an alarm has occurred.
- To Arm, Disarm, or Force Bypass from the Master Console the user must be have Authority in **ALL** partitions, and be Global in at least 2 partitions. You will be prompted for only the partitions the user is assigned global access. Device address must be programmed as "Global".

The following is a typical display:

```
SYSTEM  12345678
STATUS  RRNNA*B
```

Possible status indications include:

A	Armed Away	**R**	Ready	**F**	Fire Alarm
S	Armed Stay	**N**	Not Ready	**P**	AC Power
M	Armed Maximum	**B**	Bypass/ Ready	**L**	Low System Battery
C	Comm Failure	*****	Alarm		
I	Armed Instant	**T**	Trouble		

To obtain more information regarding a particular partition, enter **[*] + Partition No. (e.g., [*] + [4])**. This allows viewing only of that partition. In order to affect that partition, the user must use a code that has access to that partition.

Also, in order for a user of any partition to log on to Partition 9 to view the status of all partitions, that user must have access to all partitions. Otherwise, access is denied.

The following is displayed for a fault condition on Zone 2 (Loading Dock Window) on Partition 1 (Warehouse) when a user logs on from a keypad on Partition:

```
WHSE DISARMED
HIT * FOR FAULTS
```

Pressing [*] causes the following display to appear at Partition 1's keypad(s):

```
FAULT  002  LOADING
DOCK WINDOW
```

Additional zone faults are displayed one at a time. To display a new partition's status, press [*] + Partition No.

- The Armed LED on a Master keypad is lit only if all partitions have been armed successfully.
- The Ready LED is lit only if all partitions are "Ready to Arm."
- The Ready LED is lit if only one partition is armed.
- Neither LED is lit if only some partitions are armed and/or only some partitions are ready.

Press [*] + [0] or [*] + [9] to return to the master partition. Otherwise, if no keys are pressed for 2 minutes, the system automatically returns to the master partition

The sounder on a Master keypad reflects the sound of the most critical condition on all of the partitions. The priority of the sounds, from most to least critical, is as follows:

1. Pulsing fire alarm sounds
2. T4 CO alarm sounds
3. Steady burglar alarm sounds
4. Trouble sounds (rapid beeping)

Silence the sounder by pressing any key on the Master keypad or a keypad on the partition where the condition exists.

A Master keypad uses the same panics as Partition 1. Master keypad panics are sent to Partition 1, and will activate on Partition 1. Therefore, panics must be programmed for Partition 1.

Section 4: Installation

This section describes the procedures for mounting and wiring the control panel and all the peripheral devices.

NOTE: All references in this manual for number of zones, number of user codes, number of access cards, and the event log capacity, use the VISTA-250BPT's features. See *SECTION 1: General Description* for the table listing the differences between the VISTA-128BPT and the VISTA-250BPT control panels.

Mounting the Control Cabinet

1. Before mounting the circuit board, remove the metal knockouts for the wiring entry that you will be using. **DO NOT ATTEMPT TO REMOVE THE KNOCKOUTS AFTER THE CIRCUIT BOARD HAS BEEN INSTALLED.**
2. Using fasteners or anchors (not supplied), mount the control cabinet to a sturdy wall in a clean, dry area that is not readily accessible to the general public. The back of the cabinet has 4 holes for this purpose.

UL

To provide certificated burglary service for UL installations, refer to the special requirements and *Figure 3 Cabinet Attack Resistance Considerations* to follow. For UL Commercial Burglary installations that require ATTACK RESISTANCE, use the cabinet included in the COM-UL Commercial Enclosure.

Installing the Cabinet Lock

1. Remove cabinet door, then remove the lock knockout from the door. Insert the key into the lock.
2. Position the lock in the hole, making certain that the latch will make contact with the latch bracket when the door is closed.
3. When correctly positioned, insert supplied lock clip on the inside of the cabinet into the slots on the lock cylinder. Use ADEMCO Lock # K4445V1.

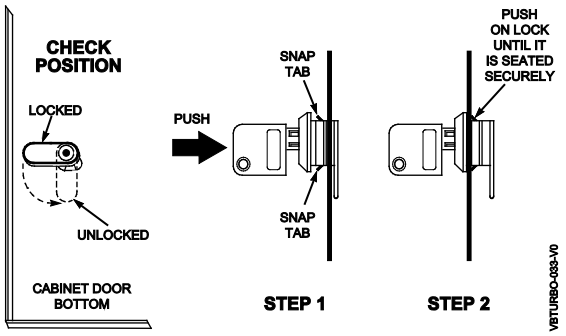


Figure 2: Installing the Lock

Mercantile Premises Listing Guidelines

- The panel door must be supervised. Mount the clip-on tamper switch (supplied) to the cabinet's right side wall as shown in the diagram 3-2 below, and wire it to one of the hardwire zones.
- Use a bell with a tamper-protected housing such as the ADEMCO AB12M. The bell housing's tamper switch and inner tamper linings must also be wired to the hardwire zone.
- Assign the tampers' hardwire zone to a burglary partition. Program the hardwire zone for day trouble/night alarm (zone type 5) when only one burglary partition is used. Program it for 24-hr. audible alarm (zone type 7) when more than one burglary partition is used.

ULC

24-Hour audible alarm (Zone types 6 and 7) is not approved for ULC application.

- All wiring between the bell and panel must be run in conduit. Remaining wires do not need to be run in conduit.
- All wiring that is not run in conduit must exit from the knockout openings on the bottom or back of the cabinet.
- All unused knockouts must be plugged using the disc plugs and carriage bolts (supplied), as indicated in the diagram below.
- Fasten the cabinet door to the cabinet back box using the 18 one-inch-long Phillips-head screws (supplied) after all wiring, programming, and checkout procedures have been completed.

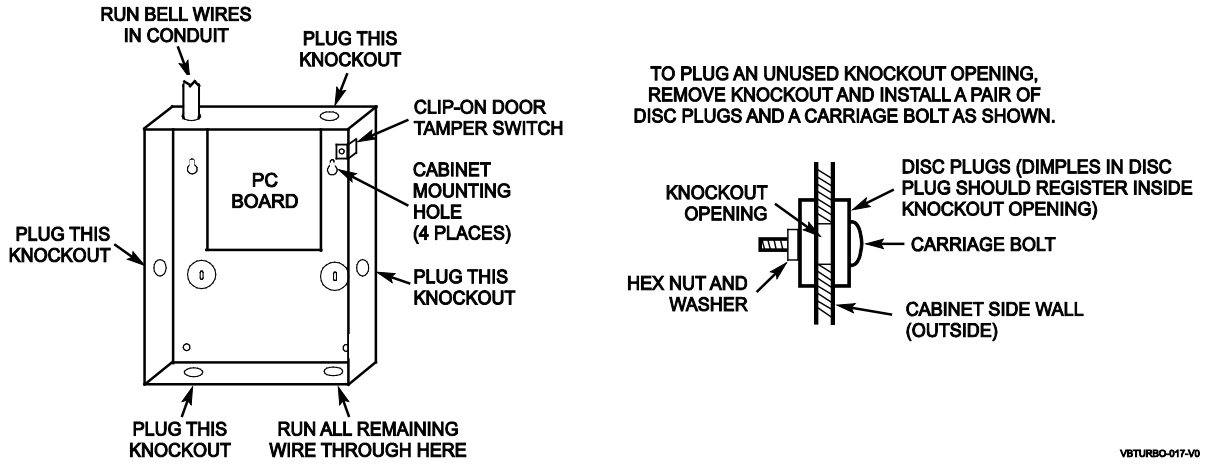


Figure 3: Cabinet Attack Resistance Considerations.

Mercantile Safe and Vault Listing Guidelines

- Follow the guidelines given above for Mercantile Premises listing.
- Mount a shock sensor such as the System Sensor ASC-SS1 to the control's back box. Follow the manufacturer's instructions for proper sensor mounting. This sensor also must be wired to a hardwire zone.
- For safe and vault applications, a UL Listed contact must be used inside the cabinet through one of the knockouts for pry-off tamper purposes. This sensor also must be wired to a hardwire zone.

Installing the Control's Circuit Board

1. Hang the three mounting clips on the raised cabinet tabs. Refer to *Figure 4* (Detail B).
   Make sure the clip orientation is exactly as shown in the diagram to avoid damage. This will also avoid problems with insertion and removal of the PC board.
2. Insert the top of the circuit board into the slots at the top of the cabinet. Make certain that the board rests in the slots as indicated (Detail A).
3. Swing the base of the board into the mounting clips and secure the board to the cabinet with the accompanying screws.

NOTES:

- Make certain that the mounting screws are tight. This ensures that there is a good ground connection between the PC board and the cabinet.
- Dress field wiring away from the microprocessor (center) section of the PC board. Use the loops on the left and right sidewalls of the cabinet for anchoring field wiring using tie wraps (Detail C). These steps are important to minimize the risk of panel RF interference with television reception.

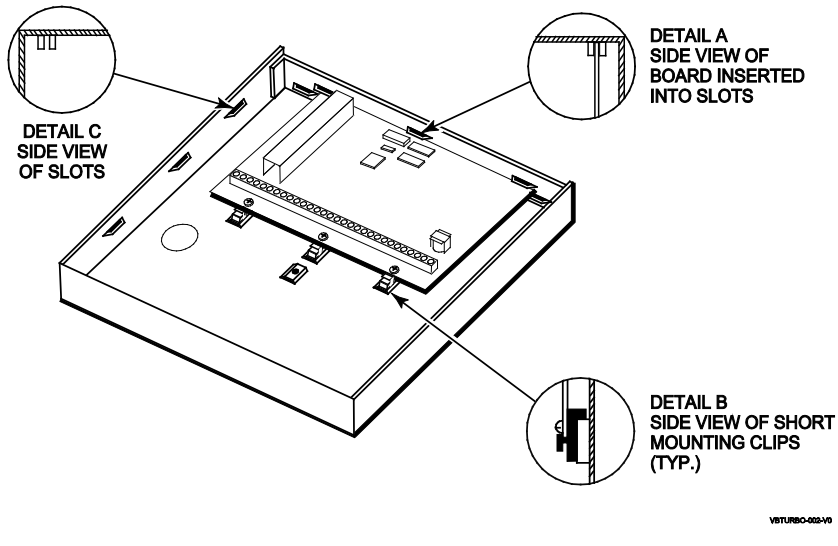


Figure 4: Mounting the PC Board

Installing ECP Devices

Supports up to 31 addressable devices (00-30), keypads, RF receivers, relay modules, etc. All devices programmable to be Supervised (Zone 8XX), refer to the *Program Guide* for programming procedure.

NOTE: You may need to use an auxiliary power supply if the 750mA aux. output is exceeded. See the "Supplementary Power Supply for Additional ECP Devices" section.

ECP Wire Run Length/Gauge Table (Unshielded)

Alpha Keypad	
Wire Gauge	**Length**
#22 gauge	450 feet
#20 gauge	700 feet
#18 gauge	1100 feet
#16 gauge	1750 feet

Touch Screen (AUI)	
Wire Gauge	**Length**
#22 gauge	150 feet
#20 gauge	240 feet
#18 gauge	350 feet
#16 gauge	550 feet

4204/4204CF Relay Boards	
Wire Gauge	**Length**
#22 gauge	125 feet
#20 gauge	200 feet
#18 gauge	300 feet
#16 gauge	500 feet

5881/5883 RF Receivers	
Wire Gauge	**Length**
#22 gauge	220 feet
#20 gauge	N/A
#18 gauge	550 feet
#16 gauge	N/A

ECP Wire Run Length/Gauge Table (Conduit/Shielded)

Alpha Keypad	
Wire Gauge	**Length**
#22 gauge	225 feet
#20 gauge	350 feet
#18 gauge	750 feet
#16 gauge	875 feet

Touch Screen (AUI)	
Wire Gauge	**Length**
#22 gauge	75 feet
#20 gauge	120 feet
#18 gauge	175 feet
#16 gauge	225 feet

4204/4204CF Relay Boards	
Wire Gauge	**Length**
#22 gauge	62 feet
#20 gauge	100 feet
#18 gauge	150 feet
#16 gauge	250 feet

5881/5883 RF Receivers	
Wire Gauge	**Length**
#22 gauge	110 feet
#20 gauge	N/A
#18 gauge	225 feet
#16 gauge	N/A

Devices maybe daisy chained. However, if the limits above are exceeded, sluggishness or lack of response may be experienced.

Devices must be homerun to the control panel

NOTE:

DI meters a minimal voltage spike on return data to the panel (i.e. button press), otherwise during idle state it reads 0VDC.

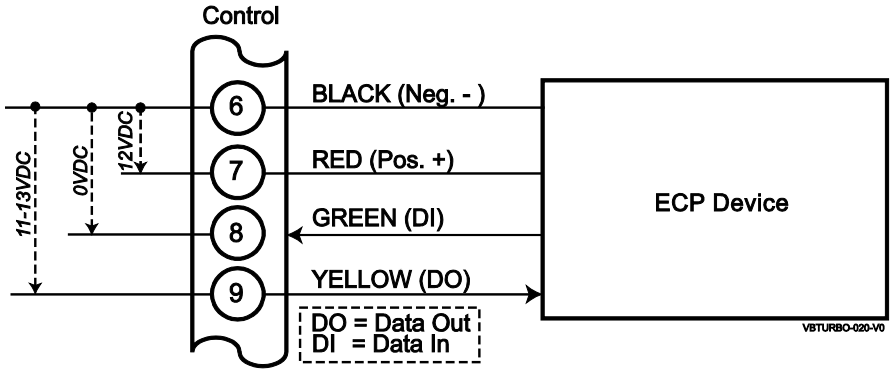


Figure 5: ECP Connections and Voltage Requirements

Wiring and Troubleshooting

If an ECP device is not working, verify the following:

- Programming has been properly configured (devices enabled in *93 Device Programming).
- Addressing of the ECP device has been configured properly.
  a. Device dipswitches addressing
  b. Software programmable addressing (i.e. keypad addressing by pressing 1 and 3 at the same time)
- Wiring is correct (i.e. DO and DI are not reversed).
- ECP voltages are correct (*see Figure 5* above for voltage requirements).

  NOTE: Constant voltage (≥ 1vdc) on DI (green) causes no response from device.
- Devices using an external power source require a common ground to the control panel.

Supplementary Power Supply for Additional ECP Devices

When the control's auxiliary power load for all devices exceeds 750mA, you can power additional keypads from a regulated 12VDC power supply (e.g., ADEMCO AD12612 (1.2A)). Use a UL Listed, battery-backed supply for UL installations.

Connect the additional keypads as shown in *Figure 6*, using the keypad wire colors shown. Be sure to observe the current ratings for the power supply used.

- Make connections directly to the screw terminals as shown in *Figure 6*.
- Be sure to connect the negative (–) terminal on the power supply unit to terminal 7 (**–**) on the control.

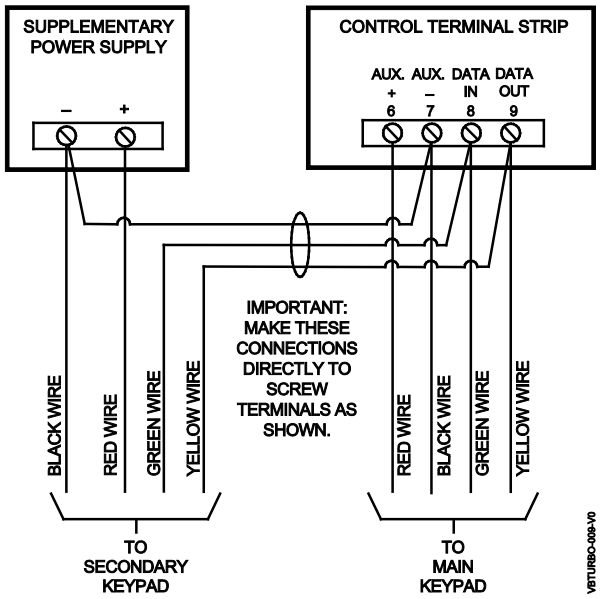


Figure 6: Using a Supplementary Power Supply

Installing the Keypads

1. Determine wire gauge by referring to the Wire Run Length/Gauge table above.
2. Wire keypads to a single wire run or connect individual keypads to separate wire runs. The maximum wire run length from the control to a keypad, which is homerun back to the control must not exceed the lengths listed in the table.
3. Run field wiring from the control to the keypads (using standard 4-conductor cable of the wire gauge determined in step 1).
4. Connect the keypad(s) to terminals 6, 7, 8, and 9 on the control board, as shown in *Figure 6*.

VOICE KEYPAD NOTES:

- Refer to the Alpha Vocabulary list found in the *#93 Menu Mode* in the *Programming Guide* for list of the words annunciated by the 6160V.
- The 6160V keypad is not to be used in SIA installations.

- The length of all wire runs combined, regardless of the wire gauge, must not exceed 2000 feet when unshielded quad conductor cable is used (1000 feet if unshielded cable is run in conduit, which acts a shield, or if shielded cable is used).
- If more than one keypad is wired to one run, then the above maximum lengths must be divided by the number of keypads on the run (e.g., the maximum length is 225 feet if two keypads are wired on a #22 gauge run).

Addressing the Keypads

The keypads do not operate until they are physically addressed **and** enabled in the system's *Device Programming (in the #93 Menu Mode)*.

- Set each keypad for an individual address (00-30) according to the keypad's instructions.
- Set an alpha keypad for address 00 and other keypads for higher addresses (00 and 01 are enabled in the system's default program).

By default, any keypads set for address 02 and above will appear blank until they are enabled in the system's program.

- Each keypad must be set for a different address.

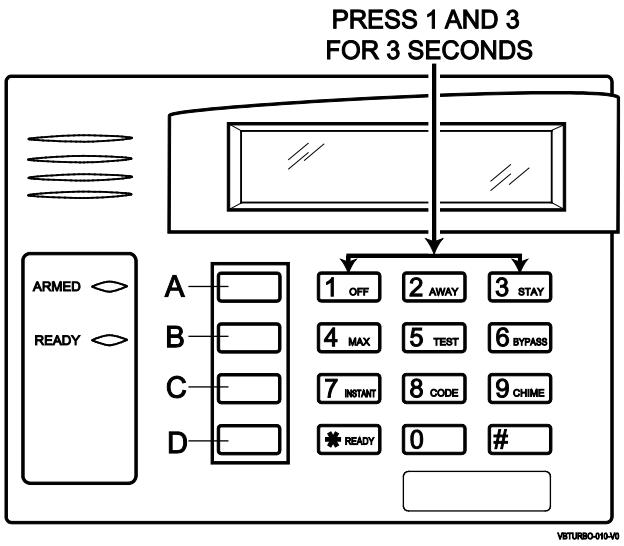


Figure 7: Keypad Addressing

Do not set any keypads to address 31 (non-addressable mode). They will interfere with other keypads (as well as other devices) connected to the keypad terminals.

Wireless Zone Expansion

UL The 5881ENHC RF Receiver, 5869 Holdup Switch Transmitter and 5817CBXT Wireless Commercial Household Transmitter are listed for UL Commercial Burglary applications. Not all other RF receivers and transmitters are listed for UL Commercial Burglary applications.

ULC Wireless devices are not ULC Listed and cannot be used for ULC Installations.

The following table lists the receivers that may be used and the number of zones they support.

Compatible 5800 Series Receivers

Commercial	
Receiver	**Zones**
5881ENHC	up to 250
5883H	Up to 250

Residential	
Receiver	**Zones**
5881EN-L	Up to 8
5881EN-M	Up to 16
5881EN-H	Up to 250

RF System Operation and Supervision

The 5800 RF system operation has the following characteristics:

- The receiver responds to a frequency of 345MHz.
- The receiver has a nominal range of 200 feet.
- Supervised transmitters send a supervisory signal every 70-90 minutes.

  Zones 988 (2nd receiver) and 990 (1st receiver) are used to supervise the RF reception of both receivers. The reception is supervised for two conditions:1.The receiver goes "deaf" (does not hear from *any* transmitter) within a programmed interval of time (defined by program field 1*30).

2. Proper RF reception is impeded (i.e., jamming or other RF interference). The control checks for this condition every 45 seconds.

UL A response type (05 Day/Night) must be programmed for zones 990 (1st receiver) and 988 (2nd receiver) for UL installations.

- The 5881ENHC receiver contains front and back tampers that permit its use in commercial burglary installations.
- You may only mount the 5881ENHC its own plastic housing. Otherwise, the receiver constantly reports a tamper condition.

- The control checks the receiver connections about every 45 seconds. The receiver supervisory zone is 8 + 2-digit receiver device address (for example, Device address 05 = supervisory zone 805).

  NOTE: This zone must be programmed with a response type (e.g., type 05 Day/Night Trouble) before it supervise the connection to the receiver.

- Use two identical receivers to provide either a greater area of coverage or redundant protection. They must be set for different addresses.

NOTES:

- No more than two receivers can be installed.
- If the receivers installed do not contain the same wireless transmitter capacity (see table above), the panel will only support a total number of zones corresponding to the receiver with the lowest transmitter capacity.
- Any zone from 1 to 250 can be used as a 5800 Series wireless zone, with the exception of zone 64 (reserved for a wireless keypad supervision)

RF System Installation Advisories

UL The 5827 and 5804BD are not UL Listed and are not intended for use in UL Listed applications.

- Place the receiver in a high, centrally located area. Do not place it on or near metal objects. This will decrease the range and/or block transmissions.
- Install the RF receiver at least 10 feet from the control or any keypads, to avoid interference from the microprocessors in these units.
- If dual receivers are used:
  a. They must be at least 10 feet from each other, as well as from the control panel and remote keypads.
  b. Each receiver must be set to a different device address. The receiver set to the lower address is considered the 1st RF receiver for supervisory purposes.
  c. The House IDs must be the same.
  d. Using two receivers *does not* increase the number of transmitters the system can support (249 zones using the 5881ENHC, plus a wireless keypad).

Receiver Installation

5881ENHC High Wireless Receiver

Take note of the address you select for the RF receiver, as this address must be enabled in the system's Device Programming in the #93 Menu Mode.

1. Mount the receiver, following the advisories stated previously.
2. Set the DIP switches in the receiver for the address **(01-07)**. See *Figure 9*.
   Make sure the address setting is not being used by another device (keypad, relay module, etc.).
3. If installing a 5881ENHC, install a flat-head screw (supplied) in the case tamper tab as shown in *Figure 8*. When the receiver is pried from the wall, the tamper tab will break off and remain on the wall. This will activate a tamper switch in the receiver and cause generation of a tamper signal.
   NOTE: This signal will also be generated when the receiver's front cover is removed.
4. Connect the receiver's wire harness to the keypad terminals (6, 7, 8, and 9). Plug the connector at the other end of the harness into the receiver.
5. Refer to the Installation Instructions provided with the receiver for installations regarding antenna mounting, commercial settings, etc.

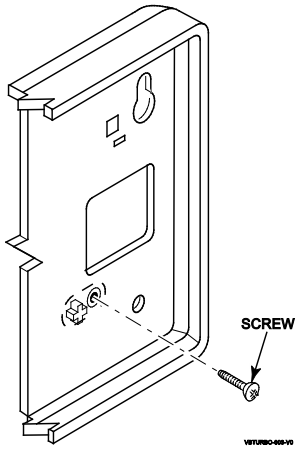


Figure 8: Installing the 5881ENHC with Tamper Protection

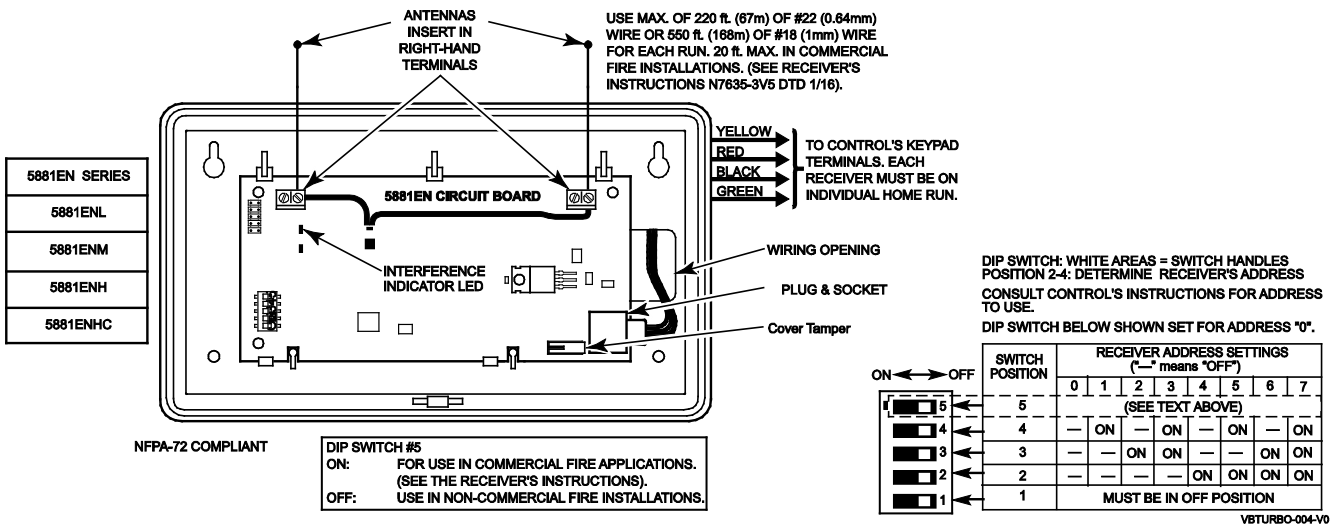


Figure 9: 5881ENH(C) RF Receiver (Cover Removed)

5883H High Wireless Receiver

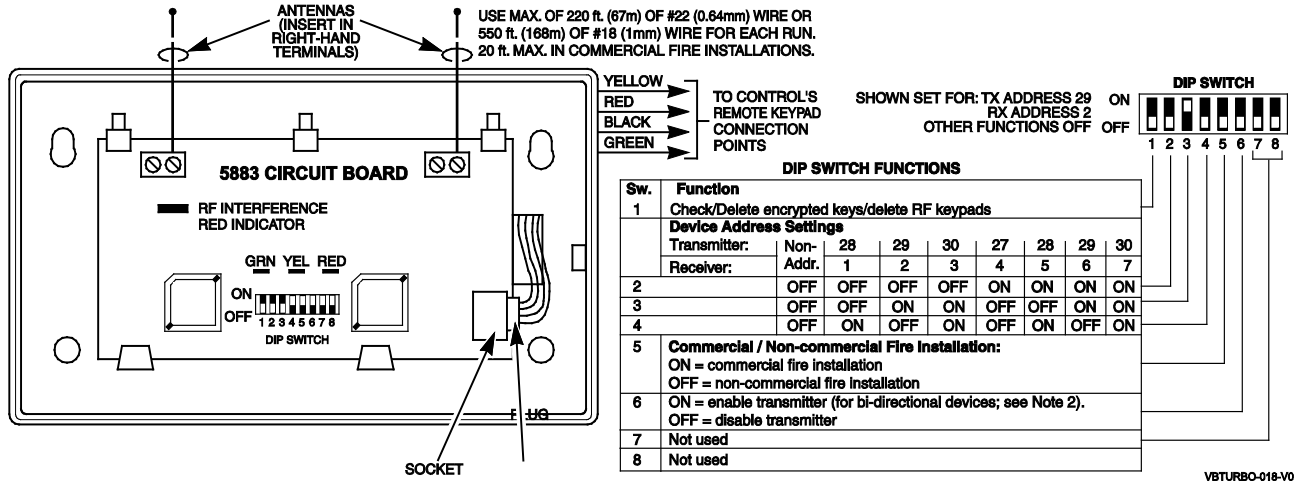


Figure 10: 5883 RF Receiver (Cover Removed)

Addressing and Bidirectional Setup

Installation of this module is necessary only if you are using a 5800 series wireless bi-directional device.

The address for the Transmission Module must be enabled in the control's *Device Programming* in the *#93 Menu Mode* as a keypad and then assigned to a partition.

1. Mount the receiver, following the advisories stated previously.
2. Connect the module's wire harness to the keypad terminals (6, 7, 8, and 9). Plug the connector at the other end of the harness into the module.

3a. Using dipswitches 2-4 set the module for the appropriate address.
Make sure the address setting is not being used by another device (keypad, relay module, etc.).

3b. Enable bidirectional status by turning dipswitch 6 on.

4. Enable the receiver and transmitter in the panel's *93 panel programming:

Transmitter	28	29	30	27	28	29	30
Receiver	1	2	3	4	5	6	7

The transmitter address corresponds with the set receiver address using the table above. (Ex. if receiver is set to address one, then the transmission module (bidirectional) is address 28).

Program the 5883H receiver address on the selected address using the table above as an "RF Expander"; program the transmitter address as an "Alpha Console" in device programming.

5. Refer to the Installation Instructions provided with the receiver for installations regarding antenna mounting, commercial settings, etc.

House ID Sniffer Mode

This mode applies only if you are using a wireless keypad (e.g., 5827) or bi-directional devices (e.g., 5804BD). Use the House ID Sniffer mode to make sure you do not choose a House ID that is in use in a nearby system. The House ID must be programmed for the receiver in *Device Programming* in the *#93 Menu Mode*.

To enter House ID Sniffer mode, enter your **Installer Code + [#] + [2].**

The receiver now "sniffs" for any House IDs in the area and displays them. Keep the receiver in this mode for 2 hours. Use a House ID that is not displayed. Exit the Sniffer mode by entering your **Installer Code + OFF**.

As Sniffer mode effectively disables RF point reception, Sniffer mode **cannot** be entered while any partition is armed.

5800 Series Transmitters Setup

5800 Series transmitters have the following characteristics:

- Transmitters have built-in serial numbers that must be enrolled in the system using the *#93 Menu Mode Programming*, or input to the control via the downloader.
- Some transmitters, such as the 5816 and 5817, can support more than one "zone" (referred to as loops or inputs). Each loop must be assigned a different zone number.
- For button-type transmitters (wireless keys), such as the 5834-4, you must assign a unique zone number to each individual button used on the transmitter.

Transmitter Input Types

All transmitters have one or more unique factory-assigned input (loop) codes. Transmitters can be programmed as one of the following types:

Type	Description
RM (Input Type 02, RF Motion)	Used for applications using multiple motion detectors that may fault and restore simultaneously. This may cause some restore signals to not be received. It automatically restores the zone to ready after a few seconds, even if the restore report is not received from the transmitter. **NOTES:** • The fault and restore may happen very quickly, which may prevent a fault for this zone from showing on the keypad. • Sends periodic check-in signals, as well as fault and low-battery signals. • The transmitter must remain within the receiver's range. • *If using RF Motion with a door/window type transmitter, only loop 1 may be used.*
RF (Input Type 03, (Supervised RF)	Sends periodic check-in, fault, restore, and low-battery signals. The transmitter must remain within the receiver's range.
UR (Input Type 04, (Unsupervised RF)	Sends all the signals that the RF type does, but the control does not supervise the check-in signals. The transmitter may therefore be carried off-premises.
BR (Input Type 05, Unsupervised Button RF)	Sends only fault signals. Do not send low-battery signals until they are activated. The transmitter may be carried off-premises.

Transmitter Supervision

Supervised RF transmitters send a check-in signal to the receiver at 70–90 minute intervals. If at least one check-in is not received from each supervised transmitter within a programmed period (field 1*31), the "missing" transmitter number(s) and "CHECK" or "TRBL" are displayed. Unsupervised RF transmitters may be carried off the premises.

Some transmitters have built-in tamper protection, and annunciate a "CHECK" or "TRBL" condition if covers are removed.

If a loss of supervision occurs on a transmitter programmed for Fire, it reports in Contact ID as a Fire Trouble (373), not Loss of Supervision (381), to the central station.

Transmitter Battery Life

Batteries in the wireless transmitters may last from 4 to 10 years, depending on the environment, usage, and the specific wireless device being used. Factors such as humidity, high or low temperatures, as well as large swings in temperature may all reduce the actual battery life in a given installation.

The wireless system can identify a true low battery situation, thus allowing the dealer or user of the system time to arrange a change of battery and maintain protection for that point within the system.

Button-type transmitters (e.g., 5834-4) should be periodically tested, as these transmitters do not send supervisory check-in signals.

To test the transmitters using the Transmitter ID Sniffer mode and the Go/No Go Test Mode, see *SECTION 10: Testing the System* for the procedures.

Compatible 5800 Series Transmitters

Door/Window Contacts

		Input Type(s)
5800MICRA	3/4" Mini Recessed Contact	RF, UR
5800RPS	Wireless Plunger Contact	RF, UR
5811	Thin Door/Window Contact	RF, UR
5814	Ultra Small Mini Transmitter	RF, UR
5815	Door/Window Contact	RF, UR
5816	Door/Window Contact	RF, UR
5816-OD	Outdoor Contact/Transmitter	RF, UR
5817XT	Three Zones Universal Transmitter	RF, UR
5817CBXT	Commercial Transmitter (5817XT with Supervised input)	RF
5818MNL	Recessed Door Transmitter	RF, UR
5820L	"Slim" Door/Window Contact	RF, UR

Glass Break & Shock Processors

5819	Shock Processor (No built in shock sensor)	RF, UR
5819 WHS/BRS	Shock Processor with built in shock sensor.	RF, UR
5853	Wireless Glass Break (Audio and Shock detection)	RF, UR
5800SS1	Wireless Glass Break (Shock only detection)	RF, UR

Motion Detection

5800PIR-OD	Outdoor (Drive Way) Motion	RF, UR, RM
5800PIR	Interior Motion	RF, UR, RM
5800PIR-RES	Residential Interior Motion	RF, UR, RM
5800PIR-COM	Commercial Interior Motion	RF, UR, RM
5800PIR-RT	5800PIR-Res with Tamper	RF, UR, RM

Panic Devices

		Input Type(s)
5802WXT	One-Button Personal Panic Transmitter	RF, UR
5802WXT-2	Two-Button Personal Panic Transmitter	RF, UR
5869	Hold-Up Switch/Transmitter	RF, UR

Fire Detection

5806W3	Photoelectric Smoke Detector	RF
5808W3	Photoelectric Smoke Detector with built in Heat sensor	RF
5809FXT	Fixed Temperature Heat Detector	RF
5800CO	Carbon Monoxide Detector	RF

Wireless Keys & Keypads

5834-4	Four-Button Wireless Key	BR
5828	Wireless Fixed LCD Keypad	N/A
5828V	Wireless Fixed LCD Keypad with Bidirectional Voice	N/A

Specialty Devices

5800RL	Wireless Relay	RF, UR
5800RP	RF Repeater	RF
5800WAVE	Bi-Directional Siren	RF, UR
5821	Temperature and Flood Sensor	RF
5822T	Tilt Sensor	RF, UR
5870API-GY/WH	Indoor Asset Protection	RF
5800C2W	Hardwired to Wireless Converter	RF, UR

Input type UR is unsupervised and used with caution.

AlarmNet Communicators Connected to the ECP

The control can support an AlarmNet ECP Communicator, which connects to control panel's keypad terminals. All messages programmed for transmission via the phone lines may also be sent via the Communicator. These messages are transmitted in Contact ID format regardless of the format programmed for the control in fields ∗45 and ∗47.

We recommend that, if possible, you use Contact ID for the main dialer. If Contact ID is not used, certain types of reports are not sent.

ULC For ULC installations, Contact ID is the only permitted format.

Installing the ECP Communicator

1. Mount the Communicator according to the instructions that accompany the Communicator.
2. Connect the data in/out terminals and voltage input terminals of the Communicator to the control's keypad connection points, terminals 6, 7, 8, and 9. See *Figure 11*.
3. Enable the ECP Communicator as device 03 in Device Programming, assign it a device type 06 "Communications Device." (See the Programming Guide for more information.)

Supervision

The data lines between the control and the Communicator, as well as certain functions in the Communicator, can be supervised.

If communication is lost or a trouble condition occurs, both the Communicator and the control's dialer can be programmed to send a Trouble message to the central station.

NOTE: For complete information, see the Installation Instructions that accompany the Communicator.

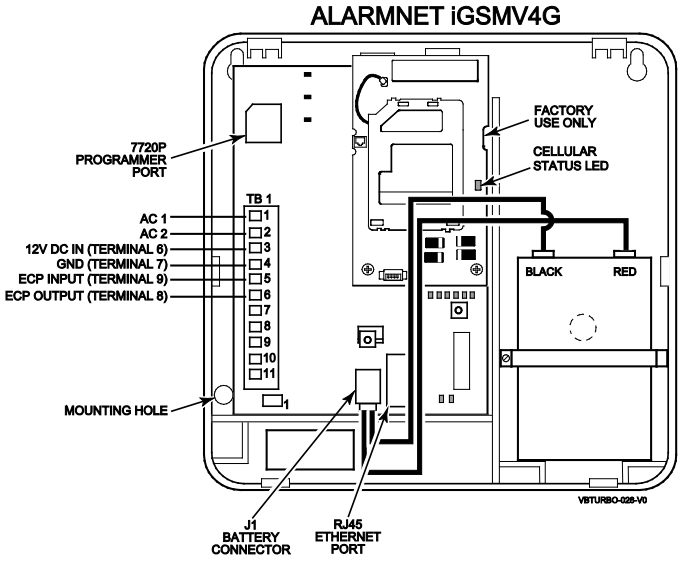


Figure 11: Wiring the Communicator to Keypad Terminals (Ex. IGSMV4G)

Trouble Messages

The following messages produce a "Check 8XX" (XX = communicator address) when supervision is enabled in the control and AlarmNet communicator:

- Power On / Reset
- Tamper
- Power Loss
- Low Battery
- Battery Charger Failure
- ECP Supervision
- Primary Communication Path Supervision
- Secondary Communication Path Supervision
- Telco Trouble
- Open/Close
- Periodic GSM Communication Test Failure
- Test

The above list is non-conclusive and new messages producing a "Check 8XX" may be added later.

Communicator Operation

The control is capable of using a phone line, AlarmNet communicator, or both to send Alarms, Troubles, System Messages, etc. to a central station monitoring facility.

Essential Programming Locations

Enabling control reporting to a central station monitoring center requires programming. The following programming locations must be programmed.

Telephone	AlarmNet Communicator
*32 – Primary Account Number (Partition Specific) *33 – Primary Phone Number *34 – Secondary Phone Number *90 – Secondary Account Number (Partition Specific)	*32 – Primary Account Number (Partition Specific) *56 – Dynamic Signaling Delay *57 – Dynamic Signaling Priority *58 – LRR CS#1 Category Enable *59 – LRR CS#2 Category Enable (Dual Reporting Only)

These programming locations enable event reporting and specific events require report codes (such as zone alarms/troubles, system events, open/close, etc.). For programming location their information refer to the *Programming Guide*.

Dialer Queue Notes

The control has a dialer/ECP radio queue of 128 messages, which consists of 37-Life Safety events (Zone types 09, 12, 14, 06, 07, 08, 16, 17, and Duress) and 91 (burg and system).

- If there are more than 37 life safety events, the burg queue will be used, however if there are more than 91 burg and system events then the life safety queue will not be used.
- When the queue is full it **cannot** accept future messages and reports an E354 to CS and any further events are lost.
- Once in the queue, messages are sent by priority of Critical then Non-Critical. If the panel makes all programmed attempts to report and fails, then the queue is emptied upon Communication Fail.

  NOTE: There is no priority WITHIN Critical events and Non-Critical Events.

- If 2*03 is enabled and the panel makes all programmed attempts to report and fails, then those events are held in the buffer. When a new event is generated the panel will again attempt to report, sending the new event and its entire buffer of old events.

Integrating an AlarmNet Communicator

The control features **Dynamic Signaling Delay** and **Dynamic Signaling Priority** message reporting when an AlarmNet Communicator is used. These options are accessed through data fields ∗56 and ∗57, respectively. The Dynamic Signaling feature is designed to reduce the number of redundant reports sent to central station.

The feature is described as follows:

Dynamic Signaling Delay (Field ∗56)

Select the time the panel waits for an acknowledgment from the first reporting path before it attempts to send a report to the secondary reporting path. Delays can be selected from 0 to 225 seconds, in 15-second increments.

NOTE: Dynamic Signaling Delay is disabled when the primary reporting path is in a fault condition.

Dynamic Signaling Priority (Field ∗57)

Select the initial reporting destination for reports, Primary Dialer **(0)** or Communicator **(1)**.

The chart below provides an explanation of how the Dynamic Signaling feature functions.

If Priority (∗57) is...	**And message is...**	**Then...**
Primary Phone No. ("0")	Acknowledged before delay expires	Report is ***removed*** from queue and ***no message*** is sent to Communicator.
	Not acknowledged before delay expires	Report is ***sent to both the Primary Phone No. and Communicator.***
Long Range Radio ("1")	Acknowledged before delay expires	Report is ***removed*** from queue and no message is sent to ***Primary Phone No.***
	Not acknowledged before delay expires	Report is sent to ***both the Primary Phone No. and Communicator.***

Additional Communicator reporting options are defined by selecting the events for each subscriber ID in fields ∗58 and ∗59. The reporting events are:

- Alarms
- Troubles
- Bypasses
- Openings/Closing
- System Events
- Test

Also, within an enabled category, the specific event must be enabled for primary dialer reporting.

NOTE: The Periodic Test Report does not follow Dynamic Signaling Priority. It is always sent to all enabled communication paths.

Dual/Split Reporting Notes

- There are two subscriber IDs programmed into the Communicator: Primary and Secondary. ∗51 Dual Reporting must be enabled for events selected in ∗59 to report to the secondary subscriber ID of the AlarmNet communicator.
- Dual reporting over the AlarmNet communicator requires two subscriber ID's programmed into the control for each partition (∗32 for Primary and ∗90 for Secondary).
- If a subscriber ID for a partition is not programmed, the panel will not report events for the partition; the events enabled in ∗58 and ∗59 for the corresponding subscriber ID in the Communicator will not be transmitted.
- The Periodic Test report does not follow Dynamic Signaling Priority. It is always sent to all enabled communication paths.

Example (Dual Reporting Enabled in ∗51)

1. Event is recorded in the control's reporting buffer.
2. Control sends report to the primary and secondary phone numbers.
3. Control sends the same message to the AlarmNet Communicator.
4. Second event is sent and the process starts over.

The first event in the queue is transmitted to both the primary and the secondary Communicator central stations before transmitting the second event.

Split Reporting Note (1∗34)

If Split Reporting (1∗34) is selected for the control, **only** events reporting to the Primary phone number will report over the AlarmNet communicator.

Installing Output Devices

The control supports up to 96 outputs. Each device must be programmed as to how to act (ACTION), when to activate (START), and when to deactivate (STOP). A total of 15 4204 relay modules may be used and supports up to 60 outputs. A total of 96 outputs is obtained using 96 4101SN's. The 4204 and 4101SN may be used in conjunction with each other, until programming the maximum of 96 outputs.

Installing a 4204 Relay Module

ULC Relay modules have not been evaluated for ULC installations.

Each 4204 module provides four Form C (normally open and normally closed) relays.

The relay module will not operate until the device address you have set the DIP switches for is enabled in the control's *Device Programming* in the *#93 Menu Mode*.

1. Set the 4204 dip switches for a device address **01-15**, refer to *Figure 12* below.
   Do not use an address being used by another device (keypads, RF receivers, etc.).
2. Mount the 4204 Module per the instructions provided with them.
3. **Connect the module's wire harness to the control (6, 7, 8, and 9). Plug the connector (other end of harness) to the module.**
   If you are mounting remotely, homerun each module to the control. Refer to the table on page 11.

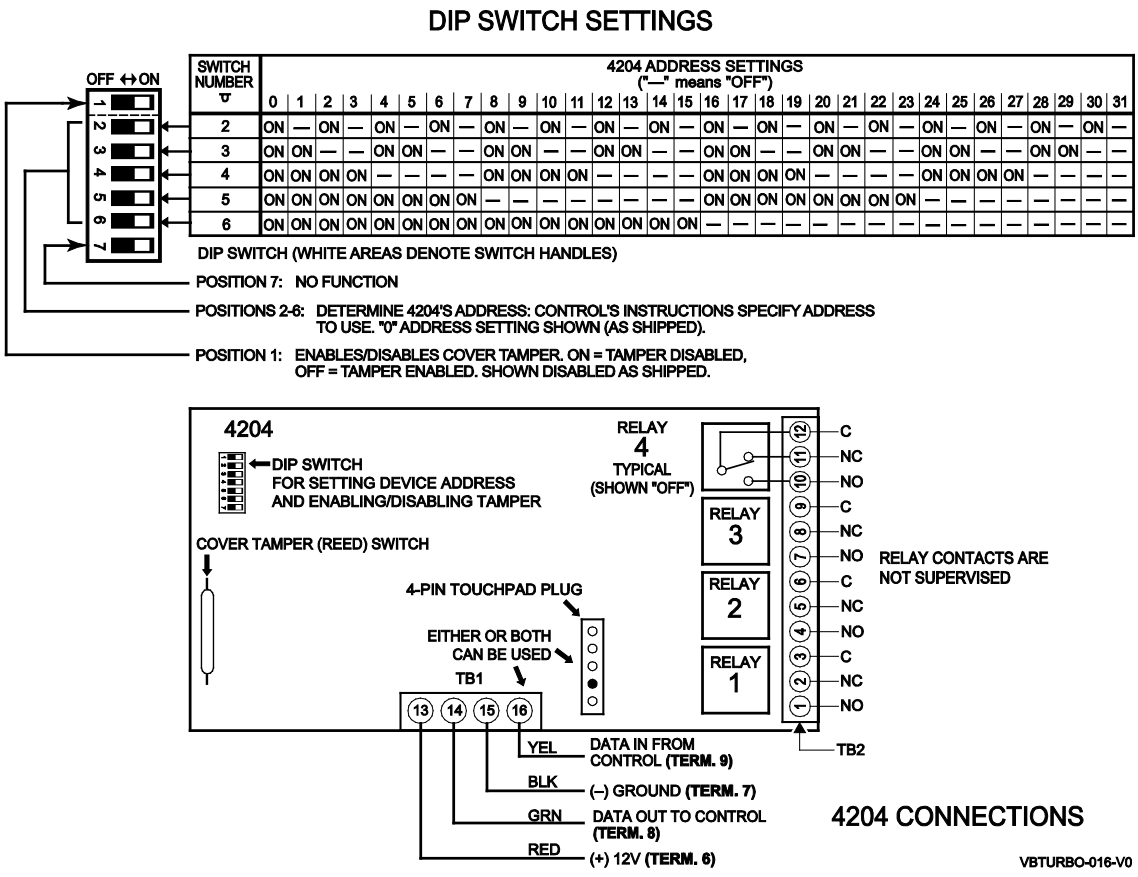


Figure 12: 4204 Relay Module

Installing the 4101SN

The 4101SN V-PLEX Single Output Relay Module is a serial number polling loop output device. The 4101SN features the following:

- Form C relay contacts rated at 2A, 28VAC/VDC with contact supervision.

The position of the relay is supervised, but not the actual external contact wiring.

- One class B/style B EOLR-supervised auxiliary input zone.
- Operating power and communication with control panels via the V-PLEX polling loop.
- Electronics mounted in a small plastic case with tamper-protected cover.

Connect the device to the polling loop, terminals 24 (+) and 25 (-). Be sure to observe polarity.

NOTE: The panel will not recognize the 4101SN until the zone associated with the device is enrolled in *93 Zone Programming. Zone must be programmed using an input type of "Serial Poll" (06); then enabling the "V-PLEX Relay" option.

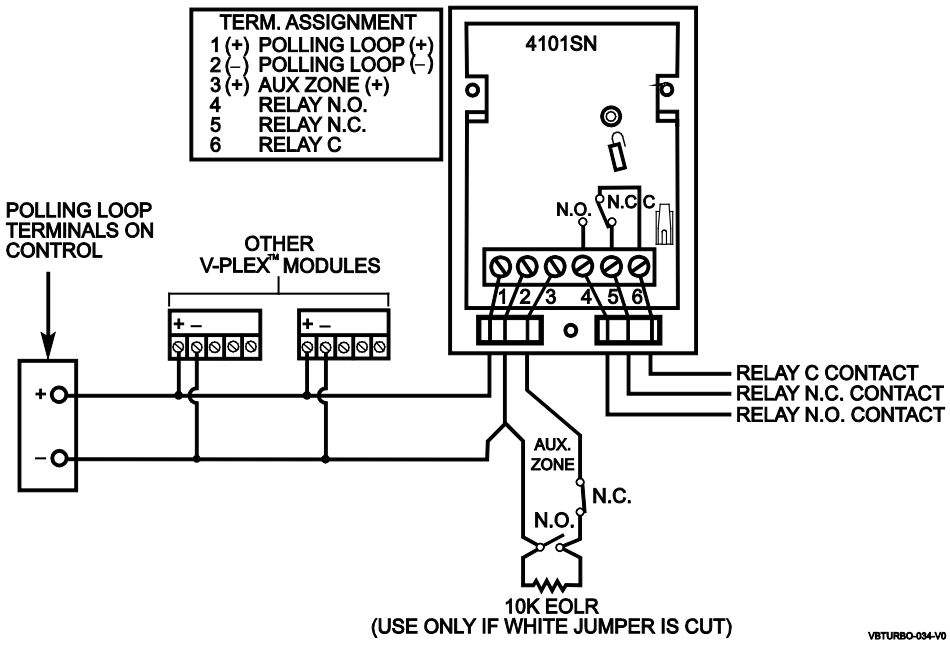


Figure 13: 4101SN Connections

Installing External Sounders

The control provides a bell circuit output for operating fire and burglary alarm notification appliances. The alarm output is rated 10VDC – 14VDC, 1.7A max., power-limited.

UL

- For Household Fire and combination Household Fire/Burglary installations, the total current drawn from the auxiliary power, polling loop, and alarm output combined must not exceed 750mA.
- For Household Burglary installations, the total current drawn from the alarm output must not exceed 1.7A.

A battery must be installed, as it supplies the current for the combined auxiliary power, polling loop, and alarm output in excess of 750mA.

The output has the following options:

- Selectable for supervision.
- Selectable for confirmation of arming ding.
- Selectable to chime when entry/exit or perimeter zones are faulted.
- Selectable for a timeout of 2-30 minutes.

UL Burglary bell circuits must be programmed for a timeout of 16 minutes or longer.

UL985 Household Fire or Combination Household Fire/Burglary Installations

For installations that must provide UL Listed protection, the total combined current drawn from the alarm output, auxiliary power output, and polling loop must not exceed 750mA in order to comply with the battery independence requirements.

UL1023 Household Burglary Installations

For Household Burglary installations, the total current drawn from the alarm output must not exceed 1.7A. A battery must be installed, as the battery supplies current from the combined auxiliary power, polling loop, and alarm output in excess of 750mA.

Non-UL Installations

For non-UL installations, the total current drawn from this output can be up to 1.7A. A battery must be installed, as the battery supplies current in excess of 750mA. Up to two 719 sirens can be used wired in parallel.

UL This control complies with National Fire Protection Association (NFPA) requirements for temporal pulse sounding of fire notification appliances.

Alarm Output Supervision

When supervision is enabled, the VISTA-128BPT/VISTA-250BPT monitors the alarm output wiring for open and short circuit faults while the output is inactive. The system provides a trouble indication (Zone 970) when an open occurs; or when a short occurs between the Bell (+) and Bell (-) terminal wiring, or between the Bell (+) terminal wiring and earth ground.

UL When supervising the bell output (zone 970), only one device can be connected to the alarm output (terminals 4 and 5) for UL and Fire installations.

The VISTA-128BPT/VISTA-250BPT indicates the trouble condition regardless of whether the system is armed or disarmed. The zone displays on the keypads, reports to the event log, and transmits to the central station (if programmed) on Partition 1. The Contact ID event code is 321, Bell Trouble. The trouble is cleared from the display by entering the user code + OFF.

Wiring the Alarm Output

The wiring of the alarm output depends upon whether you are going to supervise the output or not. Use the appropriate procedure below for your application.

UL Use only UL Listed sounding devices for UL installations.

Compatible Alarm Indicating Devices

Model Number	Device Type	Polarizing Diode
719	Compact Outdoor Siren(not UL Listed)	Yes
747	Indoor Siren	Yes
AB12M	Bell	Yes
System Sensor HR	Fire Piezo Horn	No
System Sensor P2RK, P4RK	Fire Horn/Strobe	No
Wheelock AS-121575W	Fire Horn/Strobe	No

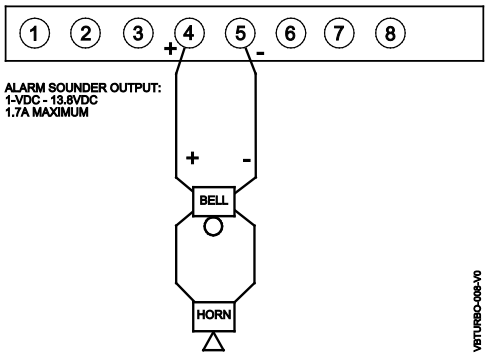


Figure 14: Wiring Polarized Fire Devices

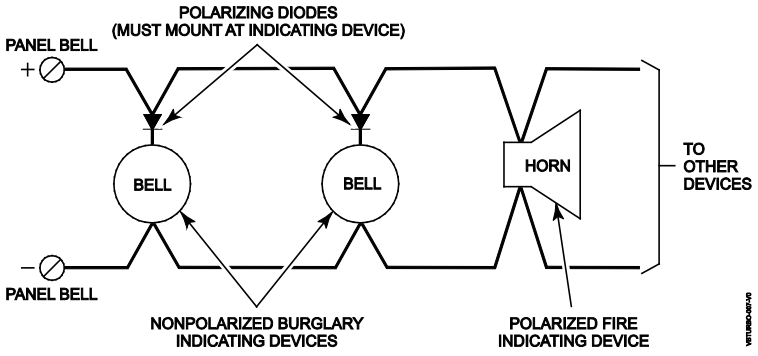


Figure 15: Wiring Nonpolarized Burglary Devices

NOTES: Positive connection for alarm sounder output sits at 6.01VDC (0vdc if Bell supervision jumper is cut, see below) and provides 14VDC at 1.7A upon activation of alarm.

IMPORTANT:
A battery must be installed, as it supplies the current for the combined auxiliary power, polling loop, and alarm output in excess of 750mA.

Supervising the Alarm Output

1. Wire polarized fire-indicating devices to the alarm output as shown in *Figure 14*.
2. Wire nonpolarized burglary indicating devices to the alarm output using a polarizing diode (two 2A diodes supplied), as shown in *Figure 15*.
3. Program Zone 970 with a response type of 05 (trouble by day/alarm by night).

   NOTE: When supervising the bell output (zone 970), only one device can be connected to the alarm output (terminals 4 and 5) for UL and Fire installations.

The minimum load on the alarm output must exceed 5mA at 12V for proper supervision operation.

UL

If a device such as a siren driver with a high-resistance trigger input (drawing less than 5mA) is used in a UL Household Fire installation, the siren driver must independently supervise siren speaker wiring.

Using a Siren Driver

1. Mount the siren driver in the panel's cabinet.
2. Wire the siren driver to the control and to the speaker(s). (See the driver's instructions.)
3. Cut the blue jumper on the upper left-hand corner of the panel's PC board.

   NOTE: Failure to cut the Blue Jumper may result in a constant trigger for the driver, subsequently causing the bell/sounder to constantly sound.
4. Program Zone 970 with no response type (00).

Disabling the Supervision of the Alarm Output

1.	Wire the devices to terminals 4 and 5, observing polarity if necessary.
2.	Cut the blue jumper on the upper left-hand corner of the panel's PC board.
3.	Program Zone 970 with no response type (00).

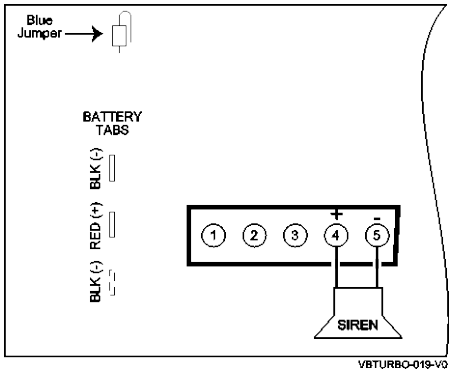


Figure 16: Disabling Bell Supervision

Telephone Line Connections

Connect the main dialer output to telephone company lines using the cable supplied.

UL The telephone line inputs have overvoltage protection in accordance with UL1459, as specified in UL985/UL1023.

The system is shipped defaulted for Contact ID format. It is the only format capable of uniquely reporting all 250 zones, as well as openings and closings for all 250 users. This requires central stations to be equipped with the Honeywell MX8000 receiver or equivalent.

To prevent the risk of shock, disconnect phone lines at the telco jack before servicing.

If the communicator is connected to a PABX, be sure it has a backup power supply that can support the PABX for 24 hours (central station) or 60 hours (remote station). Many PABXs are *not* power-backed up, and this can result in a communication failure if power is lost.

Reporting Formats

The system supports the following formats:

- ADEMCO Contact ID
- ADEMCO 10-Digit Contact ID
- 4 + 2 Express.

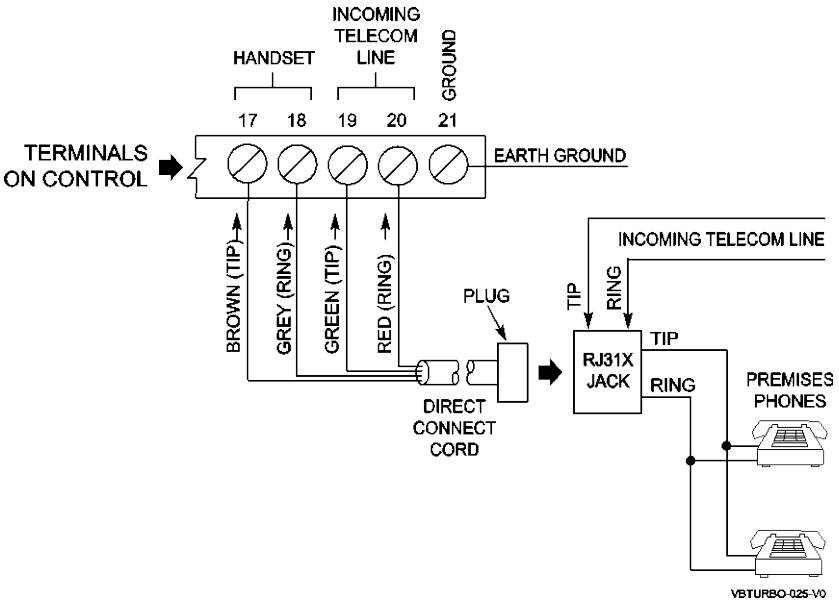


Figure 17: Telephone Line Connections

Wiring Burglary, Panic and Smoke Detector Devices to Zones 1-9

The maximum zone resistance is 100 ohms for zones 1 and 8, and 300 ohms for all other zones (excluding the 2K EOL resistor).

ULC Smoke detector devices have not been evaluated for ULC installations.

To wire burglary and panic devices to zones 1-9, connect sensors/contacts to the hardwire zone terminals (10 through 23). See *Figures 19 and 20*. Connect Normally Closed (N.C.) and Normally Opening (N.O.) devices as follows:

- Connect N.C. devices **in series** with the high (+) side of the loop. The 2K EOL resistor must be connected in series at the last device.
- Connect N.O. devices **in parallel (across)** the loop. The 2K EOL resistor must be connected across the loop wires at the last device.

  NOTE: N.O. Devices do not work with zone 09.

- Cutting the Red Jumper above terminals 10 and 11 removes supervision for zone one. **IT MUST REMAIN INTACT FOR FIRE DEVICES.** (Cutting the jumper limits the zone to N.C. wired devices only.)

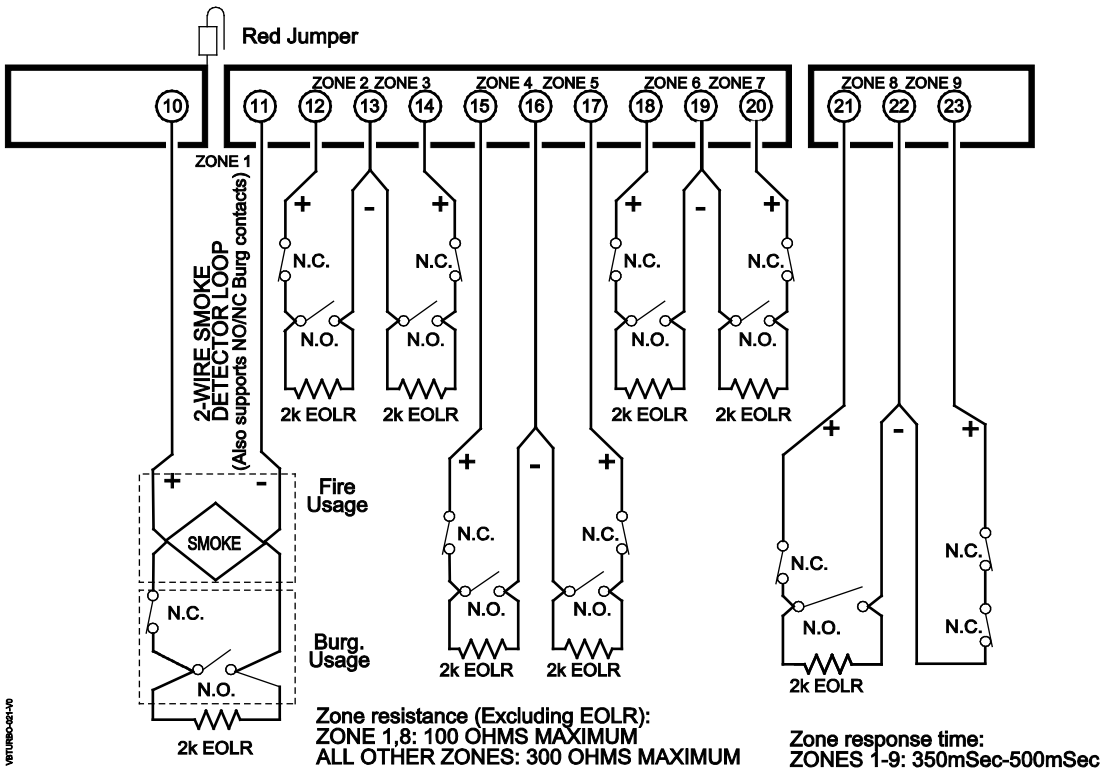


Figure 18: Wiring Connections for Zones 1-9

Zone Technical Specifications

Zone(s)	Specifications
1	Zone one is rated for 10-14VDC at 25mA. Voltages: Resistor intact: 12.9VDC Resistor removed: 13.5VDC Voltage drop: 0 for 8 seconds on this terminal to reset 2-wire Smoke Detectors.
2-7	**EOLR CONFIG:** Maximum Loop Current (Loop Short): 7.4mA Maximum Loop Voltage (Loop Open): 13.3VDC Loop Short: 0V - 1.5V - 300 ohms total resistance) Loop Normal: 4.2 - 6.8V, 1.2k - 2.6k Loop Open: 7.2V - 13.3V, 3k – Infinity Response Time: 350-500mSec Zone resistance (Excluding EOLR): 300 OHMS MAXIMUM
8	**EOLR CONFIG:** Maximum Loop Current: 9mA Maximum Loop V: 13.3VDC Loop Short: 0 - 2.2V - (0 - 300 ohms) Loop Normal: 5 - 9V (0.9k - 3.4k) Loop Open: 10V - 13.3V, 3.8k – Infinity Response Time: 350-500mSec Zone resistance (Excluding EOLR): 100 OHMS MAXIMUM Zone 8 can support 2-wire non-V-PLEX glassbreak detectors. The zone provides enough standby current to power up to 50 two-wire glassbreak detectors meeting the requirements listed below. Standby Voltage: 5VDC -13.8VDC Standby Resistance: Greater than 20k ohms (equivalent resistance of all detectors in parallel) Alarm Resistance: Less than 1.1k ohms (see note below) Alarm Current: 2mA - 10mA Reset Time: Less than 6 seconds **NOTES:** • You can use detectors that exceed 1.1k ohms in alarm, provided they maintain a voltage drop of less than 3.8 volts in alarm. • The ADEMCO ASC-SS1 detector has been tested and found to be compatible with these ratings.

Tamper Supervision for the Hardwired Zones

The system can be programmed to monitor for either an open condition or a short condition of a tamper switch on zones 1-8. End-of-line supervision is required for this option.

Wiring a Tamper Switch to Zones 1-8

The wiring of the tamper switch depends on whether the tamper switch and the sensor are normally open or normally closed.

- **If you are using a normally closed sensor,** the tamper switch must be normally open. Refer to *Figure 19* for the wiring configuration.
- **If you are using a normally open sensor,** the tamper switch must be normally closed. Refer to *Figure 20* for the wiring configuration.
- **For the normally closed sensor**, program the zone for trouble on short. **For the normally open sensor**, program the zone for trouble on open.

To wire a tamper switch on a hardwired zone, connect the EOL resistor at the last detector in the loop across the zone's terminals.

IMPORTANT: You must connect the EOL resistor at the last detector for proper operation of the tamper supervision.

NOTES:

- These zones cannot be programmed for any 24 hour zone type and that tamper supervision is only in the disarmed state. When armed the control goes into alarm.
- For zones with a response type of 9 or 16 (Fire), the tamper selection must be "0" none.

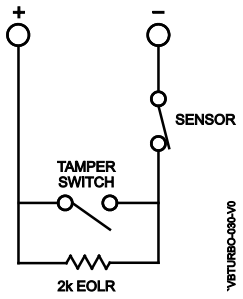


Figure 19: Wiring a Normally Closed Loop for Tamper Supervision

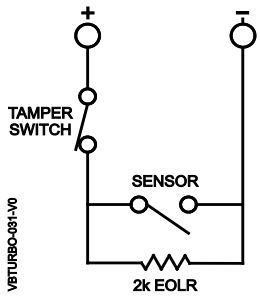


Figure 20: Wiring a Normally Open Loop for Tamper Supervision

Using 2-Wire Smoke Detectors on Zone 1

Zone 1 can support up to 16 2-wire smoke detectors.

The alarm current on zone 1 supports only one smoke detector in the alarmed state.

Compatible 2-Wire Smoke Detectors

DETECTOR TYPE	DEVICE MODEL #
Photoelectric, direct-wire	System Sensor 2W-B
Photoelectric w/heat sensor, direct-wire	System Sensor 2WT-B
Ionization w/B401B base	System Sensor 1451
Photoelectric duct detect (DH400 base)	System Sensor 2451
Ionization duct detector (DH400 base)	System Sensor 1451DH
Ionization, direct-wire	System Sensor 1100
Photoelectric w/B110LP base	System Sensor 2151

UL These smoke detectors are UL Listed for use with the VISTA-128BPT/VISTA-250BPT and are the **only** 2-wire smoke detectors that may be used.

Wiring 2-Wire Smoke Detectors to Zone 1

2K EOL resistors must be used on fire zones and must be connected across the loop wires of each zone at the last detector.

1. Select up to 16 2-wire smoke detectors from the list of compatible detectors.
2. Connect 2-wire smoke detectors across zone 1 terminals (10 and 11) as shown in *Figure 21*. Observe proper polarity when connecting the detectors.

The EOL resistor must be connected across the loop wires at the last detector.

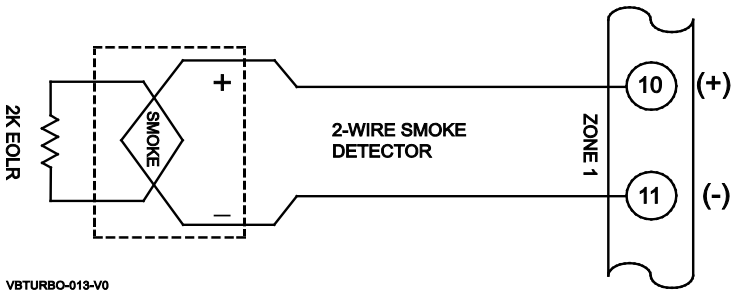


Figure 21: 2-Wire Smoke Detector on Zone 1

J7 Specifications and Usage

This control provides a trigger output which can be used for a remote keypad sounder, keyswitch (open, close, etc.) LED, and smoke detector reset. Do NOT exceed the triggers specifications below.

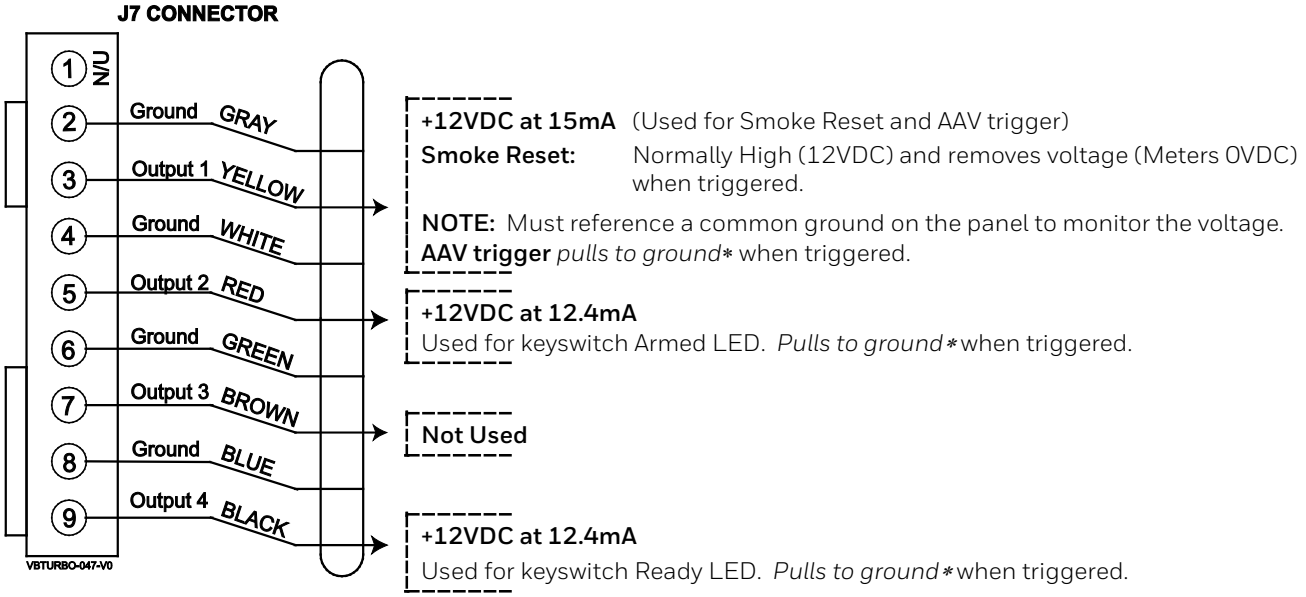


Figure 22: J7 Trigger Pin Out

* The statement "*pull to ground*" refers to the control electronically shorting the +12VDC on the trigger to ground. It can be used to active a device, such as an AAV or relay module, requiring a – negative trigger (ex. smoke reset).

Verifying Voltages:

NOTE:

When metering the trigger, you must use the auxiliary power on the control **OR** an auxiliary power supply with a common ground to the panel.

Output 1

To verify voltage place the positive meter lead on the blue wire from the J7 connector and the negative meter lead connects to auxiliary power negative or the Black wire on J7.

Output 1 responds based on the value programmed in 1*46:

1*46 = 3 (Audio Alarm Verification or AAV Trigger)

- Provides +12VDC in the normal non-triggered state.
- Triggers to ground upon kissoff of the E606 (Listen-in to follow report) for two-seconds.

1*46 = 1 (Smoke Detector Reset)

- Provides +12VDC in the normal non-triggered state. (See figure 24)
- Upon smoke detector reset (Code + 1 (off) when there is a short on a fire zone) the voltage will momentarily provide a ground, triggering the reset relay for six-seconds, allowing the smoke detector reset.
- This requires a low sensitivity relay, which you wire the smoke power through the relay.

NOTE: The short on the zone in alarm must be shorted at the zone terminals on the panel. If is not present the reset does not occur.

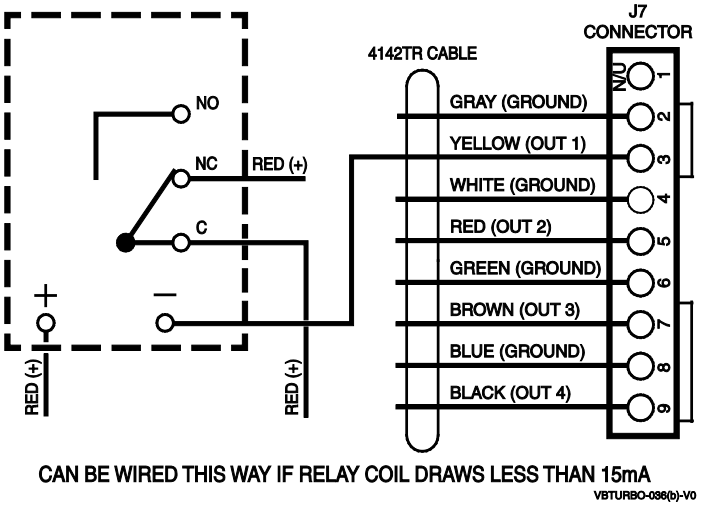


Figure 23: Low Sensitivity Relay

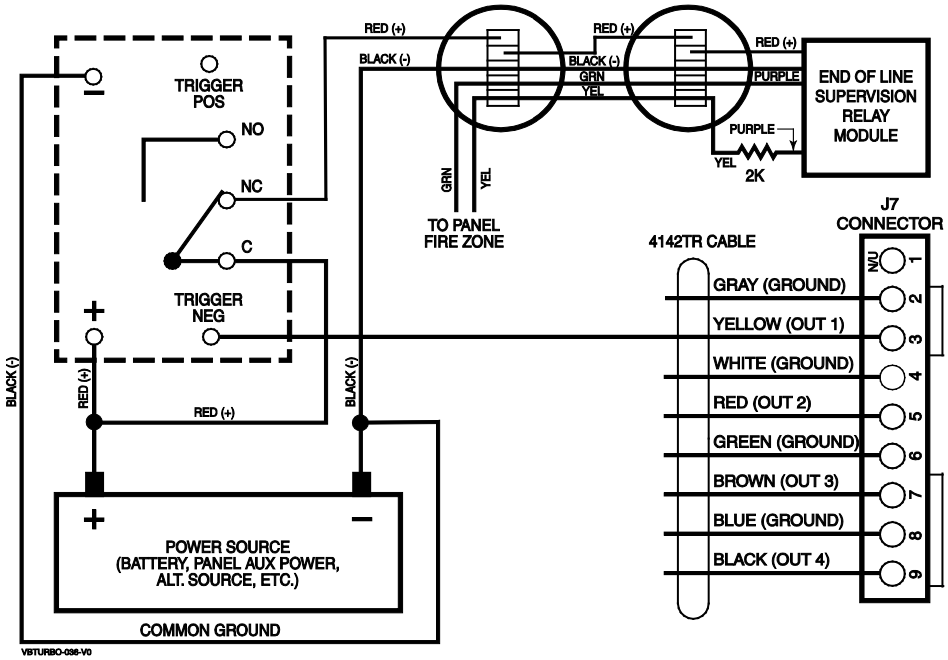


Figure 24: Smoke Reset Using Low Sensitivity Relay

Outputs 2 and 4

Place the + (positive) meter lead on the auxiliary positive terminal/wire of the power supply and the – (negative) the trigger.

- In the non-triggered state the voltage is 0VDC
- When the trigger is activated the control will apply the ground reference to the trigger and your meter reads 12VDC.
- See the *Remote Keyswitch* section below (figure 26).

4204 4-Wire Smoke Reset

This control allows you to put as many 4-wire smoke detectors as can be powered from the panel's Auxiliary Power output without exceeding the output's rating (750mA). If needed 4-wire smokes may also be powered off an external power supply. They must occupy an **EOL SUPERVISED** zone (1 – 8). You can use any UL listed 4-wire smoke detector that is rated for 10-14VDC operation and that has an alarm reset time not exceeding 6 seconds. Reset can be accomplished with a programmable relay (4204 or 4101SN) or the onboard J7 Smoke reset trigger.

NOTE: Zone 9 cannot be used for fire.

- NFPA limits the number of 4-wire smoke detectors to 18 per zone.
- Auxiliary power to 4-wire smoke detectors is not automatically reset after an alarm, and therefore must be momentarily interrupted using either the J7 smoke detector reset output trigger (figure 24) or a 4204 Relay Module.

Compatible 4-Wire Smoke Detectors

Use any UL Listed 4-wire smoke detector that is rated for 10-14VDC operation and that has alarm reset time not exceeding 6 seconds. Some compatible 4-wire smoke detectors are listed below.

Detector Type	Detector Model #
Photoelectric, direct wire	System Sensor 4W-B
Photoelectric w/heat sensor, direct wire	System Sensor 4WT-B

Wiring 4-Wire Smoke Detectors

UL Power to 4-wire smoke detectors must be supervised with an EOL device (use a System Sensor EOLR-1 EOL relay module connected as shown in *Figure 25*).

1. Select 4-wire smoke detectors (see list of compatible detectors shown previously).
2. Connect detectors (including heat detectors, if used) across terminals of the zone selected. All detectors must be wired in parallel.
   NOTE: If you are using the J7 output trigger to reset the smoke detectors, refer to *J7 Triggers section (figure 24)* for the wiring instructions.
3. Connect the EOLR at the last detector in the loop across the zone's terminals. **You must connect the EOLR across the loop wires at the last detector**.

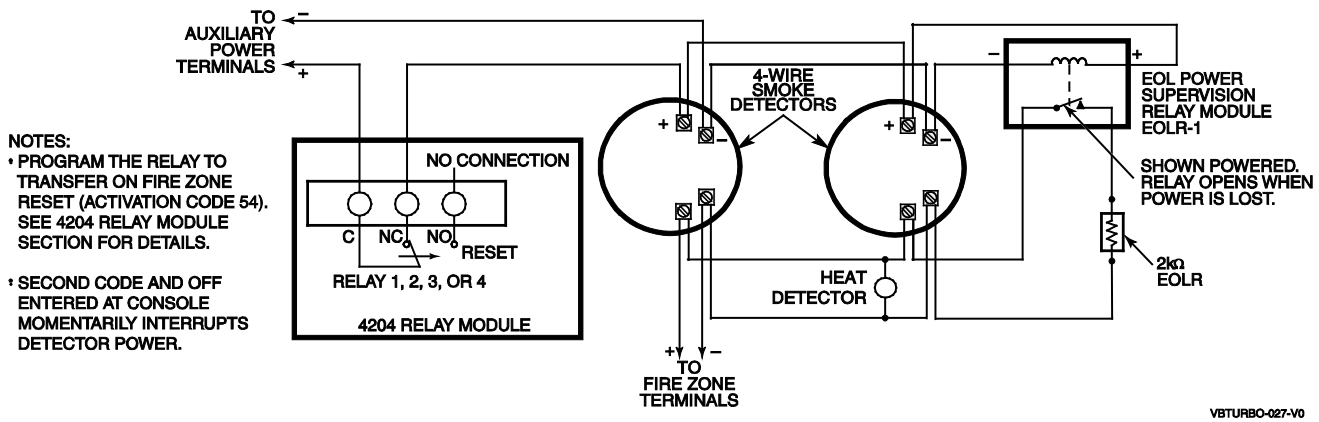


Figure 25: 4-Wire Smoke Detectors

Installing a Remote Keyswitch

A UL-Listed remote keyswitch can be used for remote arming/disarming of the burglary portion of the system and for silencing alarms. The keyswitch can operate in only one partition.

ULC Remote Arming is not a ULC Listed feature.

The keyswitch is wired across zone 7. This zone is no longer available as a protection zone. Be sure to program Zone 7 with a response type (e.g., type 10).

Operation

- A momentary short across zone 7 arms the partition in the AWAY mode, and a short held for more than 10 seconds arms the partition in STAY mode 1. A subsequent short disarms the partition.
- The keyswitch LEDs indicate the partition's status (see table below).
- A momentary short across Zone 7 silences alarm bell and keypad sounds, and disarms the system if it was armed. A subsequent short across Zone 7 clears the alarm memory indication and resets 2-wire smoke detectors (if used).

LED Indications

Green	Red	Indication
On	Off	Disarmed & Ready
Off	Off	Disarmed & Not Ready
Off	On Steady	Armed Away
Off	Slow Flash	Armed Stay
Off	Rapid Flash	Alarm Memory

The keyswitch reports as user 0, if Open/Close reporting is enabled in field *40.

Keyswitch Tamper Operation

The tamper switch need not be used for fire or UL Household Burglary installations. For UL Commercial Burglary installations, the tamper switch must be wired to a zone (zone 7 in *Figure 29*).

Program that zone for Day Trouble/Night Alarm (response type 5). When the keyswitch is removed from the wall, the tamper switch opens, causing an alarm or trouble on the zone. This also causes the control to disable keyswitch operation until the tamper is restored and the associated partition is disarmed.

Wiring for the Remote Keyswitch

1. Connect the momentary keyswitch to J7 as shown in *Figure 24*.
2. If you are using the tamper, make sure it is connected to a zone.

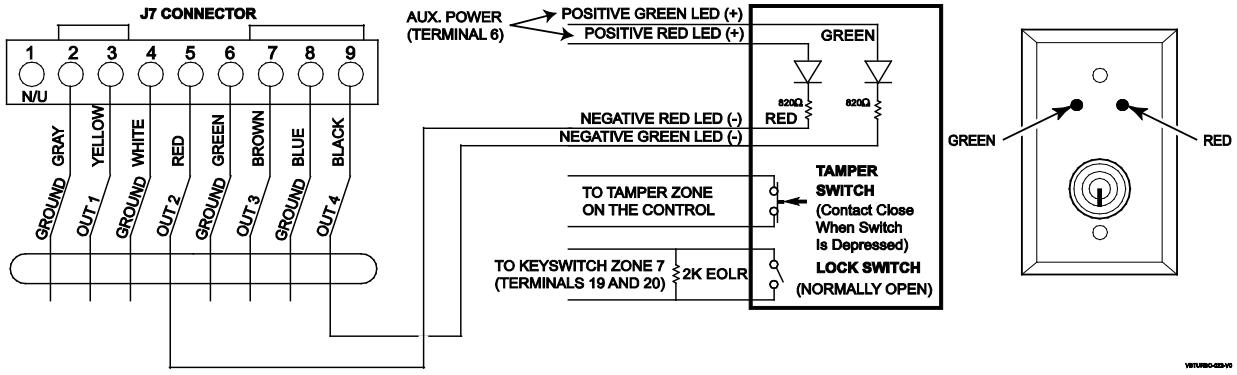


Figure 26: Remote Key Switch Wiring

Installing V-PLEX® Devices

The polling loop provides both power and data to the V-PLEX devices, and is constantly monitoring the status of all zones enabled on the loop. The maximum current draw of all devices on the polling loop cannot total more than 128mA (unless the system uses a 4297 Polling Loop Extender Module).

Devices that can be programmed via either DIP switches or the built-in unique serial number **must** be set for the serial number mode operation.

All devices on the polling loop must be wired in parallel to the [+] and [-] polling loop terminals of the control panel (24 and 25). You can wire from device to device, or have multiple branches connected directly to the control panel in a star configuration.

Compatible Polling Loop Devices

Door/Window Contacts	
4190SN	Serialized 2-Zone Expander
4193SN	Serialized 2-Zone Expander
4193SNP	Serialized 1-Zone Expander
4208SN	8 Zone V-PLEX Interface
4208SNF	8 Zone V-PLEX Class A Interface
4208U	Universal 8-Zone Expander
4939SN	Surface Mount Contact
4959SN	Aluminum Overhead Door Contact

Interior Motion Detection	
DT7500SN	V-PLEX Dual Tech PIR
IS2500SN	V-PLEX/SIM Dual Tech

Interior Glass Break Detection	
FG1625SN	Glass Break Detector

Hold Up Devices	
269SN	V-PLEX Holdup Switch

Fire Devices	
5193SD	Photoelectric Smoke Detector Device
5193SDT	Photoelectric Smoke Detector w/Heat Detector
4209U	4 zone, 2-Wire Smoke Expansion Module

Output Devices	
4101SN	Serial Number Single-Output Relay Module

Extenders/Isolators	
VPLEX-VSI	V-PLEX Short Isolator
4297	Extender Module

UL The 4297 must be powered from the control panel's Auxiliary Power Output or from a UL Listed supplementary power supply.

- For new polling loop installations, always use twisted pair wiring. In many cases, existing non-twisted pair wiring may be used, but it is more susceptible to interference from other sources, and may be problematic in installations with long wire runs or in high noise environments.
- Always locate polling loop wiring at least 6 inches (15cm) of AC power, telephone, or intercom wiring. The polling loop carries data between the control panel and the devices; interference on this loop can cause an interruption of communication. The polling loop can also cause outgoing interference on the intercom or phone lines. If this spacing cannot be achieved, shielded wire must be used. (Note that the maximum total wire length supported is cut in half when shielded wire is used.)

No more than 64mA may be drawn on any individual wire run.

V-Plex Connections and Troubleshooting

Supervision

- A short on the polling loop is indicated by a trouble on zone 997 and reports as a trouble condition only; all devices wired and programmed will result in a trouble condition. If annunciation is desired, program the zone as type 05.
- If a device on the polling loop fails (the panel cannot "see" that device), the system displays a trouble condition for all zones on that device (i.e. 4208SN).
- If it is a single zone, only that zone will display a trouble condition.
- If the panel is armed when a device fails, and the zone is a burglary zone, the system will go into alarm.

A trouble on zone 997 prevents a partition from being armed, unless all polling loop zones on that partition are bypassed.

Check 997 (polling loop short)

Indicates that there is a physical short, low voltage on the polling loop, or too much current (exceeds 128mA).

1. The panel recognizes a short when the voltage on the polling loop drops to 4.5Vdc or below.
2. Isolate this by checking voltage on the polling loop with wires connected and with all wires removed.

Limitations of V-PLEX Cable runs

The Honeywell Polling Loop has the following limitations, which apply to panels with **128mA**:

Determining the Maximum Wire Length per Polling Loop

1. Use table 1 for *Unshielded* Twisted wire and table 2 for *Shielded* cable.
2. Determine the maximum load of each device add them together to determine the maximum wire length from Tables 1 and 2.

   Example

   One 4190SN requires 2.0 mA. One 4208SN requires 27.3 mA. The total load for *one* 4208SN plus *five* 4190SNs *on the same loop* would be (27.3+ 10.0) = 37.3 ma.

3. Locate the row in the table selected in step 1 corresponding to the sum of all device currents determined in step 2.

   Example

   A total load current of 37.3 mA, corresponds to the row of (33-40) mA.

4. The maximum wire length is determined from the size, or gauge, of the wire used.

   Example

   - The maximum wire length of No. 20 gauge wire for a total device load of 37.3 mA is 4,680 feet if either unshielded (table 1) or shielded (table 2) wire is used.
   - If No. 18 gauge is used instead, the maximum allowable wire length would be 7,410 feet for unshielded cable and 6,000 feet for shielded cable.

Total Load (mA @ 11.5Vdc)	Wire Gauge			
	22	20	18	16
1-16	12,000	12,000	12,000	12,000
17-24	4,850	7,810	12,000	12,000
25-32	3,640	5,850	9,260	12,000
33-40	2,910	4,680	7,410	11,760
41-48	2,420	3,900	6,170	9,800
49-56	2,080	3,350	5,290	8,400
57-64	1,820	2,930	4,630	7,350
65-72	1,620	2,600	4,110	6,540
73-80	1,450	2,340	3,700	5,880
81-88	1,320	2,130	3,370	5,350
89-96	1,210	1,950	3,090	4,900
97-104	1,120	1,800	2,850	4,520
105-112	1,040	1,670	2,650	4,200
113-120	970	1,560	2,470	3,920
121-128	910	1,460	2,310	3,680

Table 1: Polling Loop Wiring Using Unshielded Twisted (or non-metal conduit)

Total Load (mA @ 11.5Vdc)	Wiring Guage			
	22	20	18	16
1-16	6,000	6,000	6,000	6,000
17-24	4,850	6,000	6,000	6,000
25-32	3,640	5,850	6,000	6,000
33-40	2,910	4,680	6,000	6,000
41-48	2,420	3,900	6,000	6,000
49-56	2,080	3,350	5,290	6,000
57-64	1,820	2,930	4,630	6,000
65-72	1,620	2,600	4,110	6,000
73-80	1,450	2,340	3,700	5,880
81-88	1,320	2,130	3,370	5,350
89-96	1,210	1,950	3,090	4,900
97-104	1,120	1,800	2,850	4,520
105-112	1,040	1,670	2,650	4,200
113-120	970	1,560	2,470	3,920
121-128	910	1,460	2,310	3,680

Table 2: Polling Loop Wiring Using Shielded (or metal conduit) one side of the shield to ground.

Wiring Notes and Recommendations

- Twisted, stranded, non-shielded cable is recommended. Avoid sharp bends in the wire.

- Shielded cable, running Aux power in the same jacket, and/or running wire in metallic conduit increases the capacitance of the wire run, which limits distances.
- Observe device and control requirements on serial number vs. dip-switch mode.
- Avoid running the cable near keypad wiring, intercom, or AC power lines, or anything emitting RF noise.
- If the V-PLEX device has a serial option the device must be programmed as serial.
- Shielded wire should have one end of the shield to good Earth Ground.

Using the 4297 Polling Loop Extender

The 4297 V-PLEX extender module may be used to:

1. Increase the sum of each device's load connected to the V-PLEX loop in a given system;
2. Extend the total wire length of a specific application (See limitations of V-PLEX Cable Runs);
3. Provide short circuit isolation from one loop branch to another.

Be sure to include the total current drawn on the polling loop when figuring the total auxiliary load on the panel's power supply.

NOTE: The input loop limits stated in *Figure 27* apply to *Figure 28* as well.

Voltages

The maximum load on one or more V-PLEX loops with a single supporting control panel is 128 mA.

1. If a given control panel can support a total number of devices requiring more than 128 mA, a 4297 module may be used in the manner demonstrated in *Figure 29*.
2. Each 4297 module can individually support up to 128 mA.
3. The maximum number of configurable 4297 modules is limited to 8. A DC power supply is required to furnish 50mA @ 12Vdc, plus the polling loop output current per module.

   For example if each 4297 module is to supply the maximum of 128 mA, it will require a supply current of 50+128=178 mA from a local power supply.

4. The 4297 only requires 0.1ma from the polling loop.
5. If the 4297 output is shorted, the power supply current increases to 350ma.

Wiring

The total wire length allowed at the output of a 4297 module, as well as for the control panel's V-PLEX output, is limited using Tables 1 and 2 and the procedures described above. In addition, the *sum* of the wire lengths of both the *input* and *output* of a single 4297 is also limited to 12,000 ft. of unshielded wire and 6,000 ft. of shielded wire, as indicated below.

Single 4297 to Extend Polling Loop

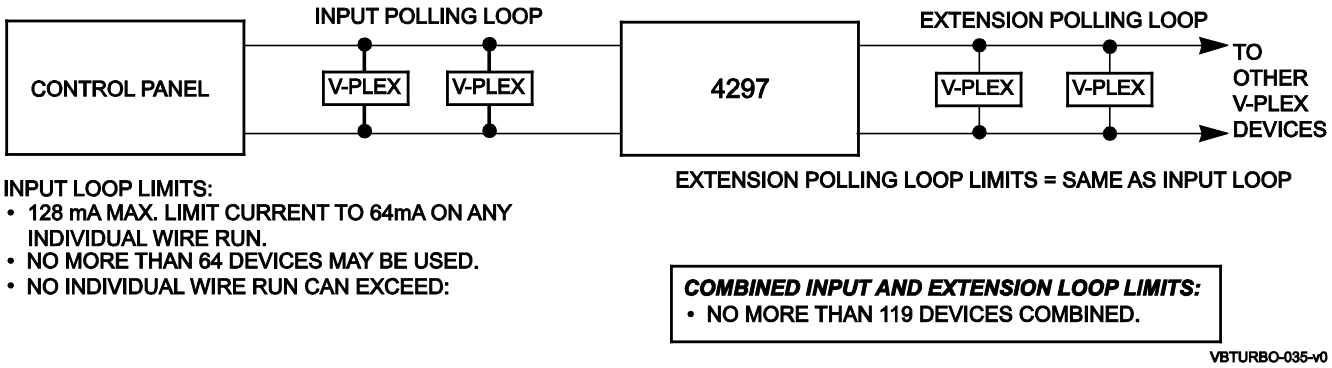


Figure 27: Polling Loop Connections Using One 4297 Extender Module

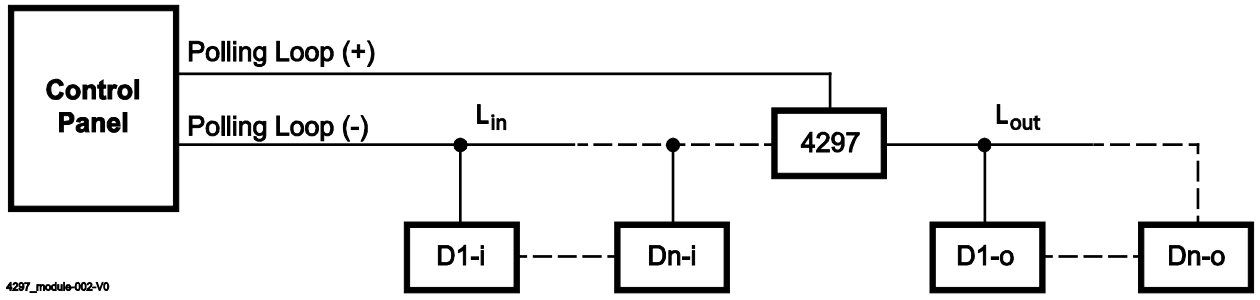


Figure 28: Single 4297 to Extend Polling Loop Calculations

D1-i + Dn-i = 128 max, or per Tables 1 & 2 above.

D1-o + Dn-o = 128 max, or per Tables 1 & 2 above.

$L_{in} + L_{out} \leq 12{,}000$ ft., unshielded, or per Tables 1 & 2 above, whichever is smaller; ≤ 6,000 ft., shielded, or per Tables 1 & 2 above, whichever is smaller.

Using Multiple 4297 Polling Loop Extenders

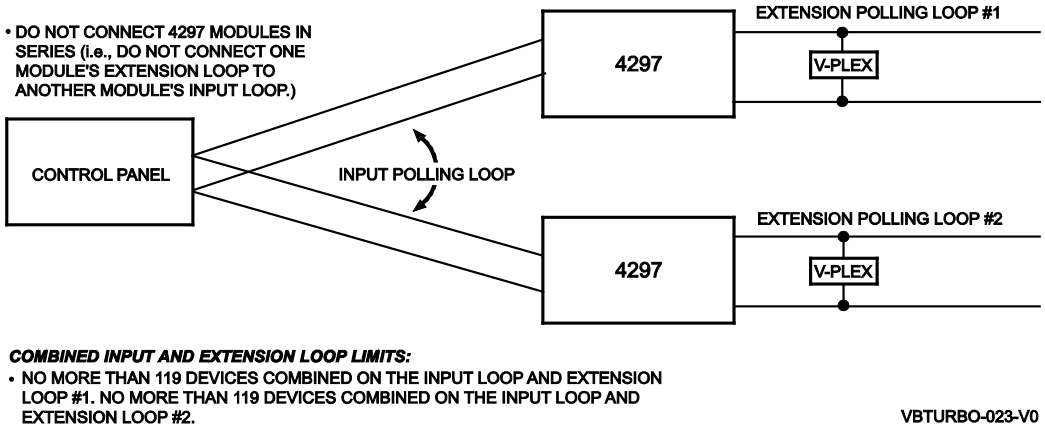


Figure 29: Polling Loop Connections Using Multiple 4297 Modules

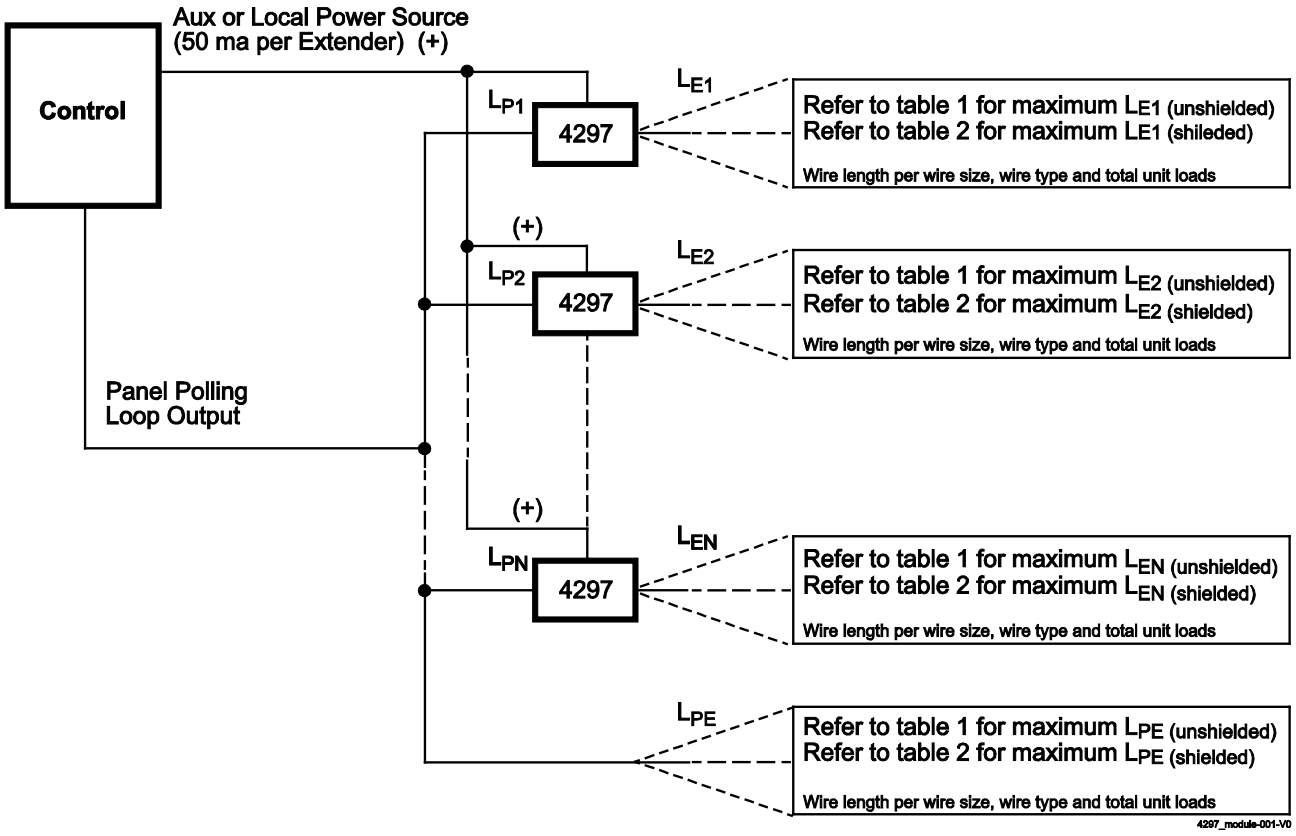


Figure 30: Polling Loop Connections Using Multiple Extender Modules Calculations

L_E =Total wire length on output side of each 4297. L_P = Total wire length on input side of each 4297.

$L_{E1} + (L_{P1} + L_{P2} + L_{PN} + L_{PE}) \leq 12{,}000$ ft. unshielded ≤ 6,000 ft. shielded.
$L_{E2} + (L_{P1} + L_{P2} + L_{PN + LPE}) \leq 12{,}000$ ft. unshielded ≤ 6,000 ft. shielded.
$L_{EN} + (L_{P1} + L_{P2} + L_{PN} + L_{PE}) \leq 12{,}000$ ft. unshielded ≤ 6,000 ft. shielded.

NOTE

The maximum number of 4297 modules which can be connected in parallel to a single system control is limited to no more than 8. The maximum wire lengths specified above and the need for the Aux or Local power source to supply 50 ma per 4297 is required.

For example, if five 4297 modules are used, the Aux or Local power source must supply (5 x 50) = 250 mA and the total system load current would be (5 x 128) +128 = 768 mA, max. Also, from the above relations;

If $(L_{P1} + L_{P2} + L_{PN} + L_{PE}) = 1000$ ft., then $L_{E1} = L_{E2} = L_{En} \leq 11{,}000$ ft., unshielded; ≤ 5,000 ft., shielded.

Using the VPLEX-VSI Short Isolator

The VPLEX-VSI Short Isolator provides short circuit isolation for V-PLEX devices. When a short occurs on a polling loop branch, it illuminates a trouble LED and isolates the defective branch from the system, reducing troubleshooting time.

1. Detects and isolates polling loop branches with complete or resistive shorts, and overload or defective VPLEX devices on initial power up;
2. Can be used to isolate loops, such as burglary devices from fire devices (see example below);
3. LED indicator reduces troubleshooting time and has low power consumption, powered directly from the V-PLEX two-wire polling loop;
4. Can be placed on any major or minor branch in any configuration on the polling loop.

The VPLEX-VSI automatically returns to normal operation and the Trouble LED is extinguished, when the trouble condition on the output side of the VPLEX-VSI is rectified.

A control panel normally reports a short on a polling loop as a trouble on zone 997. When using the VPLEX-VSI in a properly configured polling loop, this trouble condition will not occur. Instead, the zones isolated by the VPLEX-VSI will report in trouble. A few panels do not have any delay on reporting a polling loop short as a trouble. With these panels, a 997 trouble will be reported for a polling loop short. Otherwise, operation is as described above.

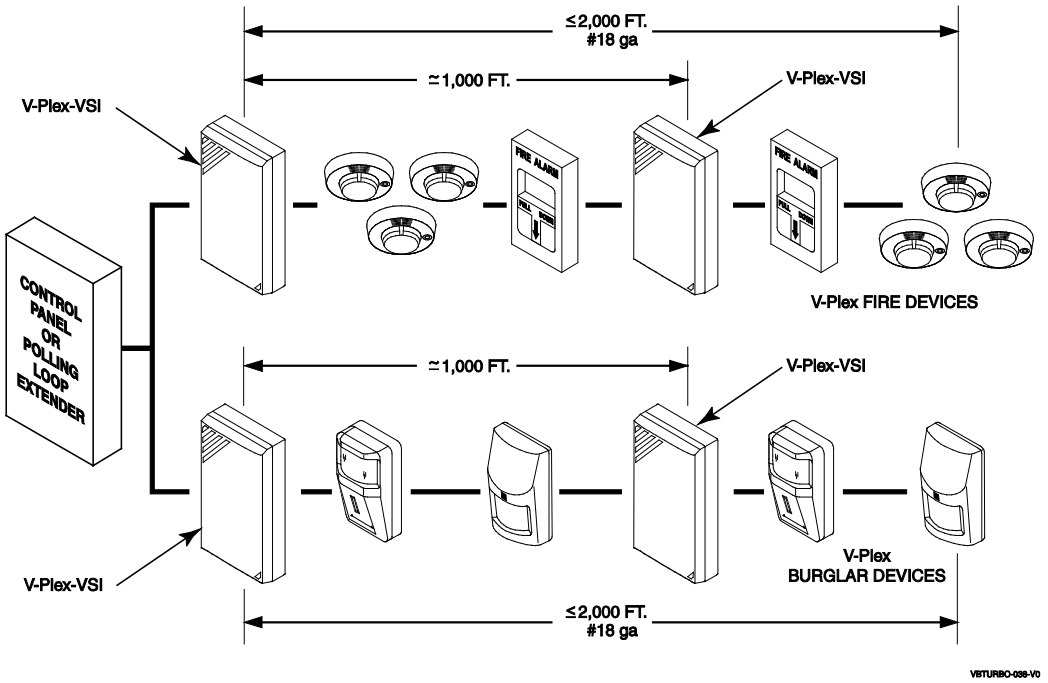


Figure 31: VPLEX-VSI Example

V-PLEX® Smart Contact Technology

Automatic suppression of fault/restores when disarmed

Smart V-PLEX sensors such as the DT7500SN, and IS2500SN polling loop motion detectors can be set to stop sending fault/restore signals while the partition is disarmed. This prevents a degradation in polling loop response from slowing down due to high bus activity in busy areas. The feature is enabled by Zone in *93 Zone Programming.

When enabled, within approximately 5 minutes of program exit, the panel will send the command to the Smart Contacts to turn off their LED and stop sending faults/restores to the system. (The DT7500SN and IS2500SN will turn off their LED unless the LED DIP switch is set to ON, in which case the LED will always remain enabled.)

Access Control Using VistaKey

The VistaKey is a single-door access control module that, when connected to the control, provides access control to the protected premises. The VISTA-128BPT/128BPTSIA supports up to 8 modules, the VISTA-250BPT supports up to 15 VistaKey modules (15 access points).

UL The VistaKey module contains three zones. These zones should ONLY be used for access control functions in UL installations. THESE INPUT ZONES ARE NOT TO BE USED FOR FIRE AND BURGLARY APPLICATIONS IN UL INSTALLATIONS.

VistaKey Features

- Each VistaKey communicates with the control via the V-PLEX polling loop.
- In the event local power to the VistaKey is lost, the VistaKey module provides backup monitoring of the access point door via a built-in V-PLEX device that is powered solely from the polling loop. It is programmed as a new type of V-PLEX device as part of the control's V-PLEX Device Programming. A serial number label is affixed to the VistaKey module for manual entry of its serial number.
- The VistaKey supports up to 500 cardholders.
- The addition and removal of VistaKey modules from the system is easily accomplished via the control's keypad.
- All configurable options for each VistaKey are accomplished via software, firmware, and nonvolatile memory, eliminating the need for PC board jumpers. The access point zone number (1-15) is set via a user-friendly, 16-position rotary switch.
- Each VistaKey provides one open-collector output trigger (sink 12mA @ 12VDC).

Mounting and Wiring the VistaKey

For detailed instructions on how to install and program the VistaKey, refer the *Installation and Setup Guide* that accompanies the VistaKey-SK.

1. Mount the VistaKey, door strike or mag lock, and card reader.
2. Mount the door status monitor (DSM) and/or request-to-exit (RTE) devices.
3. Using *Figure 32* as a reference, connect the card reader interface cable to TB3, *making the +5V or +12V connection last*.
4. Connect the leads to TB1 in the following order:
   a. All ground leads to terminals 2, 5, and 9.
   b. The DSM, (optional) RTE, and General Purpose leads to terminals 6, 7, and 8, respectively.
   c. Door strike (or mag lock) lead to terminal 10.
   d. Local +12V or +24V supply lead to terminal 1.
   e. Local +12V or +24V supply lead to the N/C relay terminal 11 (if a mag lock is being used), **OR** to the N/O relay terminal 10 (if a door strike is being used).
5. Connect the (–) polling loop and (+) polling loop leads from the control to terminals 4 and 3, respectively.
6. Set the Address Select switch to the desired access door number (1-15).
   NOTE: If a new address is desired and set the VistaKey module must be rebooted.
7. Repeat steps 1 through 6 for each VistaKey being installed.

Connecting the Card Reader

Lead from Reader	Lead Color	To VistaKey TB3 Terminal #
Green LED	Orange	1
Ground*	Black	2
DATA 1 (Clock)	White	3
DATA 0 (Data)	Green	4
+5VDC†	Red†	6
+12VDC†	Red†	7
TB-3 Terminal 5 is also a ground and may be used instead of terminal 2. Terminals 2 and 5 are a common ground. Connect to +5VDC OR +12VDC per reader manufacturer's specification.		

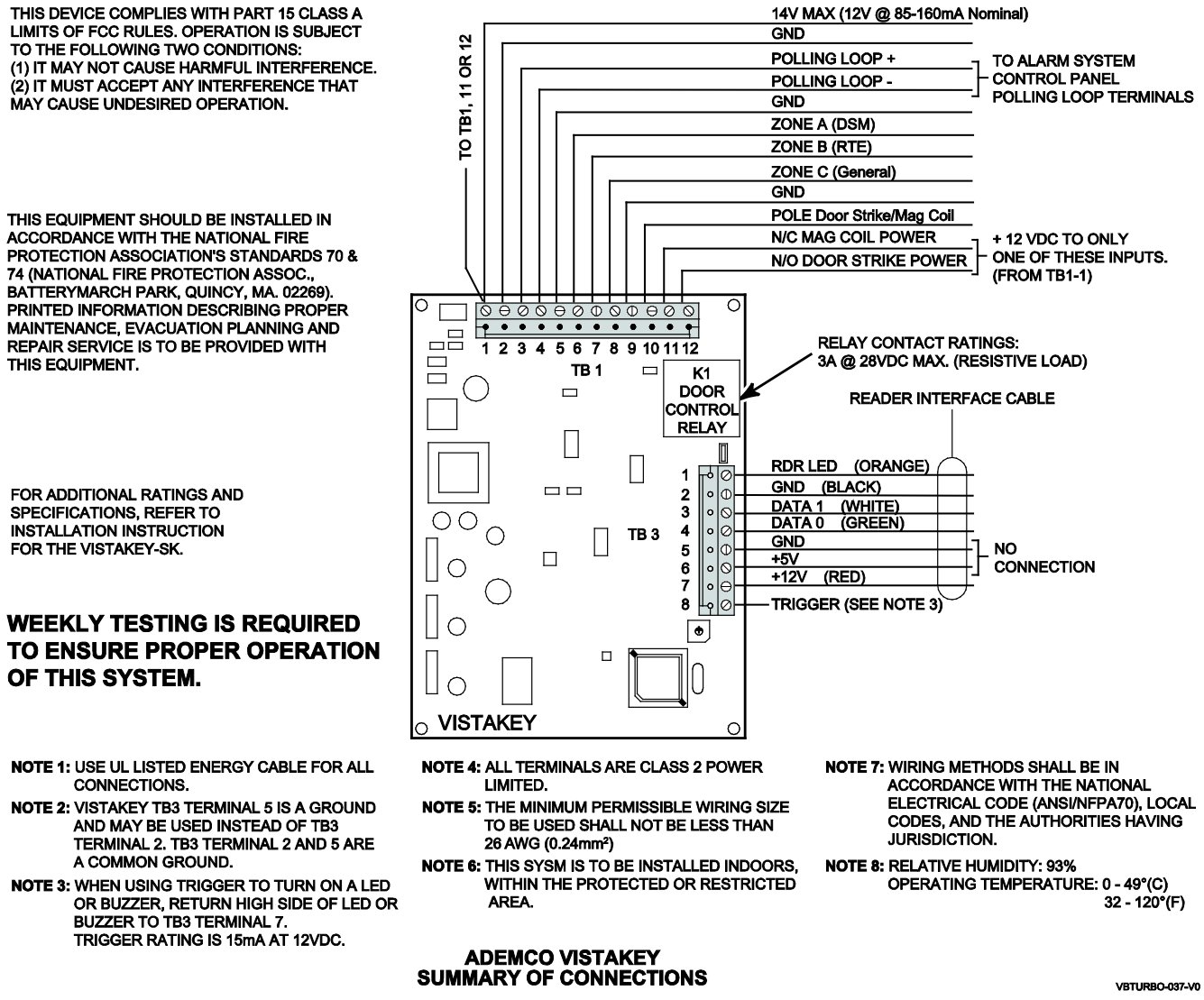


Figure 32: Wiring the VistaKey

RS-232 Connectivity

Serial Port Configuration

The enhanced serial port on the Vista Turbo Series control operates at a speed of 9600bps. Earlier Vista series panels used a speed of 1200bps. (Please note that 1200bps option has is no longer supported.) Depending on your application, you may need to adjust the configuration of your printer, home automation system or external software package to match the faster speed. Consult the documentation for your external hardware or software for directions on how to do this. In some cases you may need to contact the vendor of this external hardware or software for an update patch or driver.

Printer must be configures as 9600 Baud rate, 8 Data Bits, No Parity, and 1 Stop Bit.

Serial Port Connections

On all Vista Turbo Series panels, there are two methods of connecting to the serial (printer/automation) port:

NOTE: TB4 and J9 support WIN-PAK® and Pro-Watch®, however if you want to connect to a printer you **must** use TB4 to get the printer DSR supervision ("Printer Off Line").

1. Flying leads from terminal block TB4 to a 9- or 25-pin serial connector.
2. The VT-SERCBL cable into header J9. This connector terminates in a 9-pin serial connector.

NOTES:

- To connect this to a PC, you must use a standard straight through serial cable with a 9-pin connector on the panel end and the appropriate connector for your PC on the other end.
- The TB4 method is intended for permanent wiring, e.g. when connecting to WIN-PAK or Pro-Watch. The J9 method is ideal for direct-connect programming, where the serial connection being made is only temporary.
- When connecting via TB4, observe the TB4 pin configuration shown on the Summary of Connections label.

IMPORTANT: When connecting the VT-SERCBL cable into header J9, the red strip (pin 1) on the ribbon cable should be on the left.

NOTES:

- **TB4 and J9 cannot be used simultaneously**. If you are using one of these connection points to communicate with the panel, you MUST temporarily disconnect the other wiring.
- You cannot use WIN-PAK or Pro-Watch and the Printer at the same time.

Panel	9-Pin	25-Pin
TXD	3 (EBI-IPPS)	2 (EBI-IPPS)
	2 (All Other Configurations)	3 (All Other Configurations)
RXD	2 (EBI-IPPS)	3 (EBI-IPPS)
	3 (WIN-PAK or Pro-Watch)	2 (WIN-PAK or Pro-Watch)
RTS/DTR	8 (WIN-PAK or Pro-Watch)	5 (WIN-PAK or Pro-Watch)
CTS/DSR	4 (Printer Only)	20 (Printer Only)
GND	5 (All Configurations)	7 (All Configurations)

You cannot simultaneously use a serial printer and Home/Facility Automation.

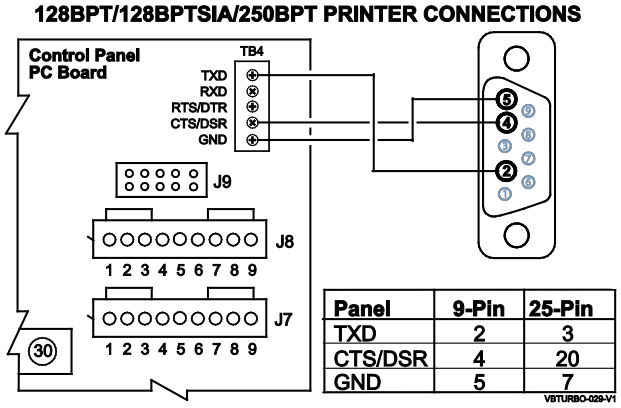


Figure 33: Printer Connections

NOTES:

- J9 and VT-SERCBL can be used for Printer output, but it does not monitor DSR voltage and printer will always show "Printer Off-Line".
- The DSR terminal of TB4 would have to be shorted to +12VDC to clear printer trouble.

Voltages

TXD to Ground sits at -11.65vdc then pulses to +4vdc while printing. (Use code #61 to print log)

Troubleshooting "Printer Offline"

1. Check for voltage on DSR Term to GND on the TB4. The printer should hold this voltage high (+8vdc) when 'Ready to Print'.
2. If the printer is not ready/offline the Printer pulls this voltage down to -8vdc. Check for pin 20 on the RS232 Cable from the printer. This should be +8vdc or more, pin 7 is Ground. During an "Offline" condition the printer will pull this to -8vdc.

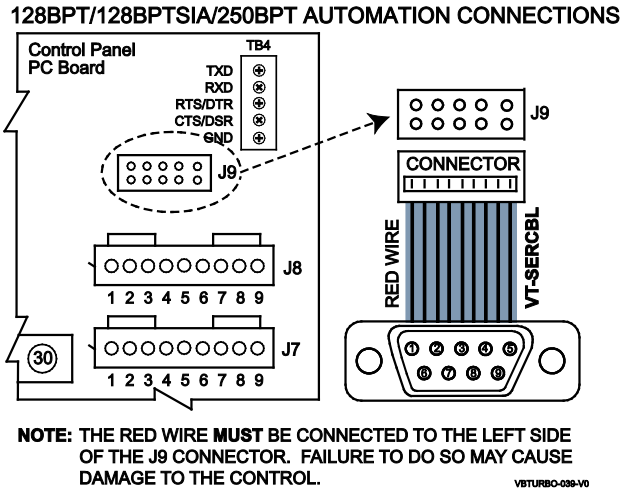


Figure 34: Automation Connections

NOTES:

- The cable between the Panel and the Automation PC is 50 ft. maximum. Shielded Cat 5 wire is recommended.
- The connected PC must be capable of receiving continuous 9600-baud data.

Testing the Transmit and Receive data at the Panel:

Receive:

On TB4 meter between RXD Terminal and GND Terminal

With no data transmitting it should sit idle at approximately -5 to -11VDC. It should quickly pulse when Automation is transmitting the data.

If this voltage exists the Automation is sending data out.

Transmit:

On TB4 meter between TXD Terminal and GND Terminal with no data transmitting it should sit idle at approximately -5 to -11VDC. When the panel is transmitting data the voltage will quickly pulse. If this voltage exists then we know that the panel is sending data out.

Connecting the Transformer

This product uses the 1361 or 1361-GT transformer (1361CN or 1361CN-GT in Canada).

NOTE: Upon a total power failure, the control unit will ignore and not transmit alarm supervisory information for a stabilization period of 120 seconds following restoration of power. Within 60 seconds at the end of the stabilization period, the control unit shall initiate the transmission of a power restoration signal code. If this report code is enabled (see report code programming in the Programming Guide), this is the report that will be sent.

UL Use 1361CN or 1361CN-GT Transformer in Canadian installations.

Power Limiting Outputs

All outputs are power-limited as per UL985/UL1023. The following table shows the maximum current that may be drawn from each output.

Output	Maximum Current Draw
Auxiliary Power	750mA
Polling Loop	128mA
Alarm Output	1.7A

For Household Fire or Combination Household Fire/Burglary Installation: The total current drawn from the auxiliary power, the polling loop, and the alarm output combined must not exceed 750mA to comply with the battery independence requirements in UL985.

For Household Burglary-Only Installations: The total current drawn from the alarm output may be up to 1.7A. A battery must be installed to supply the current of the combined auxiliary power, polling loop, and alarm output in excess of 750mA.

Failure to observe the polling loop current rating will cause polling loop malfunction. Failure to observe the auxiliary power current rating will result in a battery that does not charge properly or possibly a tripped circuit breaker.

To connect the transformer to the control, perform the following steps:

1. Connect all installed devices to the control.
2. Wire the 1361 or 1361-GT Transformer (1361CN or 1361CN-GT in Canada) to the panel (before connecting the battery) as shown in *Figure 35*.
3. Plug the transformer into a 24-hour, uninterrupted, 120VAC, and 60Hz outlet. After a few seconds, the keypad display appears.

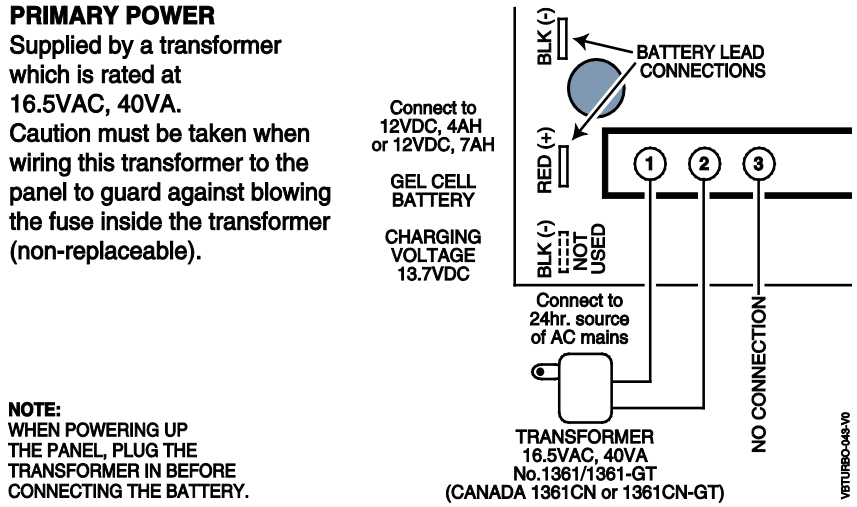


Figure 35: 1361/1361-GT (Canada 1361CN/1361CN-GT) Transformer and Battery Connections

Panel Earth Ground Connections

In order for the lightning transient protective devices in this product to be effective, the designated earth ground terminal (terminal 30) must be terminated to a good earth ground. Recommended wire gauge for the ground connection is #16 AWG; run no farther than 30 feet. The following are examples of good earth grounds available at most installations:

- **Metal Cold Water Pipe:** Use a noncorrosive metal strap (copper is recommended) firmly secured to the pipe to which the ground lead is electrically connected and secured.
- **AC Power Outlet Ground:** Available from 3-prong, 120VAC power outlets only. To test the integrity of the ground terminal, use a three-wire circuit tester with neon lamp indicators, such as the UL-Listed Ideal Model 61-035, or equivalent, available at most electrical supply stores.

The panel requires the earth ground connection for its lightning transient protection devices.

Determining the Control's Power Supply Load

Use the tables that follow to calculate the total current for the Auxiliary Power, the Alarm Output, and the Polling Loop. In each table, multiply each device's standby and/or alarm current by the number of units used.

In Table 1, enter devices used on the polling loop. Calculate total current draw on the polling loop.

In Table 2, enter devices used on Auxiliary Power. Calculate standby and alarm currents, then add to get Auxiliary Power current subtotal.

Table 1: Total Polling Loop Current Draw

Polling Loop Device	Current	# of Units	Total
Polling Loop Subtotal (Terminals 24 & 25 – 128mA) *			

*The total current cannot exceed 128mA. If total load exceeds 128mA, then a 4297 Loop Extender Module can be used. Note that the total number of points connected to the panel cannot exceed 119.

Table 2: Auxiliary Power Current Load

Device Model #	Device Current X # of Units		Total Current	
			Standby	Alarm
Auxiliary Power Subtotal (Terminals 6 & 7 – 750mA max.)				

1. In Table 3, enter devices connected to the Alarm Output. Calculate alarm currents, then add to get the Alarm Output current subtotal.

Table 3: Alarm Output Current Load

Device Model #	Device Current X # of Units		Total Current Standby	Total Current Alarm
			XXXXXX	
			XXXXXX	
			XXXXXX	
			XXXXXX	
			XXXXXX	
			XXXXXX	
			XXXXXX	
Alarm Output Subtotal (terminals 4 & 5 – 1.7A max.)				

2. In Table 4, enter the total calculated subtotals of all listed outputs from Tables 1 through 3, then add to get the combined current.

Table 4: Total VISTA-128BPT/VISTA-250BPT Current Load

	Total Current Standby	Total Current Alarm
Polling Loop Subtotal (see Table 1)		
Aux. Power Subtotal (see Table 2)		
Alarm Output Subtotal (see Table 3)		
VISTA-128BPT/VISTA-250BPT PCB Current (Includes 2-wire smoke detector loading on zone 1)	250mA	330mA
Total Current Load		

Determining the Size of the Standby Battery

The cabinet supplied with the control panel can house batteries of up to 12V, 14AH (two 12V, 7AH batteries wired in parallel). The VISTA-ULKT kit provides a cabinet that can house batteries of up to 12V, 17.2AH and that may be used with this panel. The total standby current drawn from the auxiliary power and polling loop outputs combined must be limited to 270mA when 14AH batteries are used; and to 390mA when 17.2AH batteries are used.

DO NOT use Gates batteries (sealed lead-acid type). These batteries require a different charging voltage than is supplied by the panel.

UL The maximum battery capacity in UL installations is 14AH.

UL Household Fire or Combination Household/Fire/Burglary installations require the use of a backup battery that is capable of providing 24 hours of standby time followed by 4 minutes of alarm time. UL1023 Household Burglary-only installations require the use of a backup battery that is capable of providing 4 hours of standby time followed by 4 minutes of alarm time.

Use Table 5 to determine the required backup battery capacity and use Table 6 to determine the battery model number. **A dual battery harness is supplied** that allows two batteries to be wired in parallel for increased capacity.

3. Using the total calculated from Table 4, calculate the battery capacity required for the installation.

Table 5: Battery Capacity Calculation Table

Capacity	Formula	Calculated Value
Standby Capacity	For 4-hour standby time: Total **standby current** X 4 hours X 1.2 contingency factor. For 24-hour standby time: Total **standby current** X 24 hours X 1.2 contingency factor.	
Alarm Capacity	For 4-, 5-, or 15-minute alarm time: Total **alarm curr.** X0.067 (4 min) 0.250 (15 min)	
Total Capacity	**Add standby and alarm capacities**	

4. Use the Battery Selection Table to select the appropriate battery for the installation.

Table 6: Battery Selection Table

Capacity	Recommended Battery	Comment
4AH	Yuasa NP4-12	
7AH	Yuasa NP7-12	
12AH	Yuasa NP12-12	Fits in large mercantile cabinet only.
14AH	Yuasa NP7-12	Connect two in parallel.
17.2AH	Yuasa NPG18-12	Fits in large mercantile cabinet only.

The standby battery is automatically tested for 10 minutes every 4 hours, beginning 4 hours after exiting Programming mode. In addition, entry into the Test mode initiates a battery test. The VISTA-128BPT/VISTA-250BPT also runs a 5-second battery test every 60 seconds to check if the battery is connected.

5. Connect the battery.

Section 5: Scheduling

UL

- You must program Bypass and Auto-Arm Fail reports for UL installations.
- Auto-disarming is not permitted in UL installations.
- You must not program Random Scheduling of Time Driven Events for UL installations.

ULC Scheduling is not approved for use in ULC installations.

General

The scheduling features allow certain operations to be automated, such as arming, disarming, bypassing of zones, and activating relay outputs.

The system uses time windows (a programmed period of time with a start and stop time) for defining open/close schedules, holiday schedules, user-defined temporary schedules, and access schedules for users.

Scheduled events are programmed by user-friendly menu modes of programming (#80, #81, #83, and #93 modes), explained in detail in this section. These menus take you step by step through the options.

Auto Arming

ULC Auto Arming is not a ULC Listed feature.

The system can automatically arm (AWAY Mode) a partition at the end of a pre-determined closing (arming) time window.

Auto Arming can be delayed three ways: by use of the Auto-Arm Delay, the Auto-Arm Warning, or by manually extending the closing (arming) time window with a keypad command.

The system can also automatically bypass any open zones when auto arming.

Common Lobby Notes:

If scheduling is used to automatically to arm and/or disarm partitions, the common lobby

partition does not automatically follow another partition that is programmed to arm or disarm the lobby.

The lobby must be included as a partition to be armed/disarmed and must be scheduled as the last partition armed.

If using O/C schedules the panel will auto arm in the AWAY Mode and if reporting O/C reports this reports as CID Code 403 User number 0.

NOTE: Alarm Memory will not prevent an Auto Arm.

Auto-Arm Delay (2*05)

Auto-Arm Delay provides a delay (grace period) before auto arming. It starts at the end of the closing time window.

The delay is set in 4-minute increments, up to 56 minutes in partition-specific program field 2*05. At the expiration of this delay, the Auto-Arm Warning will start.

Auto-Arm Warning (2*06)

The Auto-Arm Warning causes the keypad sounder to warn the user of an impending Auto-Arm.

The warning can be set from 1 to 15 minutes prior to the arming in partition-specific program field 2*06. During this period the keypad beeps every 15 seconds and displays “AUTO ARM ALERT.” During the last 60 seconds, the keypads beep every 5 seconds.

The panel arms at the conclusion of the Auto-Arm Warning period.

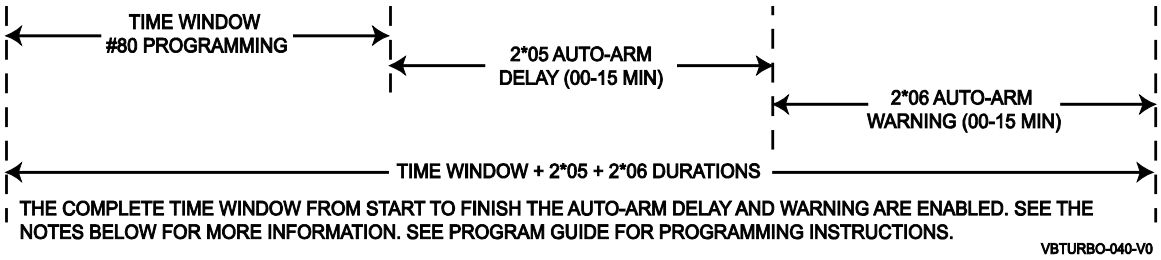


Figure 36: Scheduling Time Line

NOTES:

- 2*05 and 2*06 do not apply to "non-arming" triggers (such as relays using *Time Driven Events*).
- 2∗06 applies to Time Driven events and Open and Close schedules.

Extend Closing Window

A user can manually delay the arm (closing) time window by 1 or 2 hours. This is done by entering a keypad command **(User Code + #82)**, which then prompts the user to enter the desired extension time of 1 or 2.

This feature is useful if a user must stay on the premises later than usual.

The Auto-Arm delay and warning periods begin at the end of the extension.

Force Arm

ULC Force Arming is not a ULC Listed feature and must be disabled for ULC installations.

The Force Arm option causes the panel to attempt to bypass any faulted zones prior to auto arming (panel performs a force-arm).

This option is set in partition-specific program field 2∗08.

Auto Disarming

The system can automatically disarm a partition at the end of a pre-determined opening (disarm) time window.

The disarming time can be delayed by using the Auto-Disarm Delay feature.

Disarm Delay

Auto-Disarm Delay provides a delay before auto disarming. This delay is added to the end of the disarm time window.

The delay is set in 4-minute increments, up to 56 minutes, in partition-specific program field 2∗07.

Restrict Disarming

This option allows disarming by users only during the disarm time window and during the arming time window (in case user needs to re-enter premises after manually arming the partition).

This option is set in partition-specific field 2∗10. If field 2∗10 is set, we highly recommend setting field 2∗11, as well. This field allows the partition to be disarmed outside the arm/disarm time windows only if the partition is in alarm.

Exception Reports

This option allows the reporting of openings and closings to the central station **only** if the arming and disarming occurs outside of the predetermined opening and closing time windows. It is set in partition-specific field 2∗09.

The system can be programmed to send Failed to Open and Failed to Close reports if the partition is not armed or disarmed by the end of the corresponding time window.

Limitation of Access of Users by Time

A user's access to the system can be limited to a certain time period. Outside this time, that user's code is inactive. The system provides up to eight access schedules, each consisting of two time windows (typically one for opening, one for closing) for each day of the week and two time windows for holidays.

The access schedules are programmed in the #80 Menu Mode, and enabled when a user's access code is added to the system.

If a user tries to operate the system outside the schedule, the alpha keypad displays *"Access Denied."*

Time-Driven Events

The system can automatically activate and de-activate relays at predetermined times to turn lights or other devices on and off. The Time-Driven events can be activated at different times in relation to a time window:

- At the beginning of a time window
- At the end of a time window
- During a time window (on at beginning of window, off at end)
- At both the beginning and end of the time window (e.g., to sound a buzzer at the beginning and end of a coffee break)
- Random time at the start of the time window (occurs within 30 minutes after the start of the time window)
- Random time at the end of the time window (occurs within 30 minutes after the end of the time window)
- Random during the time window (begins within 30 minutes after the start of the time window and ends within 30 minutes after the end of the time window)

The system can perform the same actions on a daily basis, or can perform an action only once (e.g., turn on the porch light this Wednesday at 8:00 PM).

The system also provides up to 20 programmable "timers" available to the end user for the purpose of activating output devices at preset times and days.

Time Window Definitions

Scheduled events are based on time windows, (periods of time) during which an event may take place. The system supports up to 20 time windows, each defined by a "Start" time and a "Stop" time.

The windows are shared by all eight partitions, and are used when programming the various schedules (open/close, limitation of access), as well as for Time-Driven event control.

Scheduling Example

A store that has the following hours:

Monday to Friday	9am to 6pm
Saturday	10am to 4pm
Sunday	Closed
Holidays	Closed

The owner desires the following time windows to allow time for employees to arm or disarm the system:

Monday to Friday	**Open (disarm)**	8am to 9am
	Close (arm)	6pm to 6:30pm
Saturday	**Open (disarm)**	9am to 10am
	Close (arm)	4pm to 4:30pm
Sunday & Holidays	**Closed**	

For this schedule, the four time windows need to be programmed:

Window	*Start*	*Stop*	*Purpose*
1	8am	9am	Monday-Friday open window
2	9am	10am	Saturday open window
3	4pm	4:30pm	Saturday close window
4	6pm	6:30pm	Monday-Fri. close window

Using the *#80 Menu Mode*, the installer can program open/close schedules by assigning a time window to a day of the week (windows are entered as 2-digit entries)

Mon	Tue	Wed	Thu	Fri	Sat	Sun	Hol
Op/Cl	Op/Cl	Op/Cl	Op/Cl	Op/Cl	Op/Cl	Op/Cl	Op/Cl
01/04	01/04	01/04	01/04	01/05	02/03	00/00	00/00

NOTE: 00 is entered for those days on which the store is closed.

Employees can arm and disarm the system, when programmed, within the open and close time windows without causing a report to be sent to the central station (reporting by exception, field 2∗09). The system can be programmed to automatically arm/disarm in case an employee fails to arm/disarm manually (auto-arm/auto-disarm).

Open/Close Schedules Definitions

General

The open/close scheduling is controlled by one of three schedules. Each schedule consists of one time window for openings and one time window for closings.

There are three types of schedules available: Daily, Holiday, and Temporary.

Daily Schedule

Each partition can have one daily schedule consisting of one opening window and one closing window per day.

Holiday Schedule

A holiday schedule overrides the regular daily schedule on selected holidays throughout the year.

The opening and closing windows are programmed in the daily schedule, but the holidays themselves are defined in *Holiday Schedule Programming* in the *#80 Menu Mode*.

Temporary Schedule

The temporary schedule provides a method for the end user to override the daily and holiday schedules. It consists of one opening window and one closing window for each day of the week. The schedule takes effect for up to one week, after which it is automatically deactivated.

This schedule is programmed using the #81 Temporary Schedule Menu Mode.

Additional Schedules

Additional opening and closing schedules can be programmed using the *Time-Driven Event Programming*. For example, a schedule for normal store openings/closings can be programmed with a daily open/close schedule, and another open/close schedule for a lunch hour can be programmed using the Time-Driven event schedule programming.

Refer to "Time-Driven Events" later in this section for detailed information.

Open/Close Reports by Exception

The system can help reduce communication traffic to the central station by using the Open/Close Reports by Exception feature. The Open/Close by Exception option suppresses these reports from being sent to the central station if an arm or disarm is done ***within*** the expected time window. Reports are only sent if the arm or disarm occurs outside the assigned time window.

The system keeps a record of ***all*** openings/closings in its event log.

If a disarming occurs during a closing window (for example, a person who arms the system forgets something and has to re-enter), the Opening report (although outside of the opening window) will not be sent (as long as that disarming occurs within the closing window).

This option is programmed in partition-specific program field 2∗09.

Example of Open/Close Exception Reporting & Scheduling

The following chart gives an example of how the Open/Close by Exception reporting works.

6:01PM 5:59AM	6AM 9AM	9:01AM 3:59PM	4PM 6PM	6:01PM 5:59AM
Early Opening reports are sent if system is manually disarmed before opening window begins. **Early and Late Opening and Closing reports are programmable options in the Report Code Programming. They are not dependent on the programming of the Exception Reporting option.**	Opening Window No reports are sent if system is disarmed during this time window. **If an arming occurs, a Closing report is sent to the central station regardless of how the Exception Reporting option is set.**	Auto-disarm delay begins. Auto-disarm occurs after delay (if auto-disarm is enabled). Missed Opening reports are sent if manual disarming has not occurred at expiration of opening window. Late Opening reports are sent if disarm occurs after the opening window expires. Early Closing reports are sent if manual arming occurs before the closing window begins. **Missed Opening/Closing type reports are programmed in the Report Code Programming. The Exception Reporting option must be set for these to be sent.**	Closing Window No reports are sent if system is armed* during this time window. * or disarmed if user needs to re-enter premises.	Auto-arm delay begins. Auto-arm warning begins. Auto-arm occurs after warning expires (if auto-arm is enabled). Missed Closing reports are sent if manual arming has not occurred at expiration of closing window. Late Closing reports are sent if system is manually armed after the closing window expires.

Scheduling Menu Mode

The #80 Scheduling Menu Mode is used to program most of the scheduling and timed-event options. Enter **Installer Code + [#] + [8] + [0]** from the *normal* operating mode.

NOTE: Only users with an Installer or Master level user code may enter the #80 mode.

The following can be programmed while in this mode:

- Time windows
- Open/Close schedules to each partition
- Holiday schedules
- Time-Driven events (for system functions and relay activation)
- Limitation of access schedules

Some scheduling features are programmed in Data Field Programming Mode (**Installer Code + 8 0 0 0**). Some features are programmed in the #93 Menu Mode. The programming scheduling fields are listed below.

System-Wide Fields:	
*04	Enable Random Timers
1*74 –1*75	Relay timeout values
2*01-2*02	Daylight saving time options
2*11	Allow disarming outside window if alarm occurs
Partition-Specific fields:	
2*05	Auto-arm delay value
2*06	Auto-arm warning time
2*07	Auto-disarm delay value
2*08	Force-arm enable
2*09	Open/Close Reporting by Exception
2*10	Restrict disarm only during windows
#93 Menu Mode (System Group #3)	
Scheduling related report codes	

Event-driven options are programmed using *Output Programming* in #93 *Menu Mode*. Relay activation can also be Time-Driven and that those are programmed using the *#80 Menu Mode*. Refer to the *Time-Driven Event Programming* later in this section for the procedure.

Steps to Program Scheduling Options

This section contains examples of the worksheets only. For complete worksheets, see the Programming Guide accompanying this Installation and Setup Guide.

In order to use #80 Scheduling Menu Mode, use the worksheets to do the following:

1. Define time windows (up to 20)
2. Define the daily open/close schedules (one schedule per day, per partition)
3. Define the holidays to be used by the system (up to 16)
4. Define limitation of access times (up to 8 schedules)
5. Define the Time-Driven events (up to 20)

   NOTE: Temporary schedules are programmed using #81 Menu Mode.

Use #80 Scheduling Menu Mode to perform the following functions:

1. Program the time windows
2. Program the open/close schedules
3. Program the Time-Driven events
4. Program the access schedules

Scheduling Menu Structure

To program schedules, enter Scheduling Program Mode:
Installer Code + [#] + [80]. (Installer or Master level user code.)

Scheduling Program Mode can be entered only when all partitions are disarmed.

There are 6 sections of scheduling menus accessed via #80, as shown below. Entering **1** at a displayed main menu prompt selects that menu section. Enter **0** to skip a section and display the next menu option.

PROMPT	EXPLANATION
Time Window ? 1 = YES 0 = NO 0	Upon entering Schedule Menu Mode, this prompt appears. Enter **1** to program time windows. Refer to *Time Windows Programming* later in this section for detailed procedures. Enter **0** to move to the "O/C Schedules?" prompt.
O/C Schedules ? 1 = YES 0 = NO 0	Enter **1** to program opening and closing schedules. Refer to *Open/Close Schedules Programming* later in this section for detailed procedures. Enter **0** to move to the "Holidays?" prompt.
Holidays ? 1 = YES 0 = NO 0	Enter **1** to program holiday schedules. Refer to *Holiday Schedule Programming* later in this section for detailed procedures. Enter **0** to move to the "Timed Events?" prompt.
Timed Events ? 1 = YES 0 = NO 0	Enter **1** to program timed events for relay outputs, additional schedules, and other system functions. Refer to *Time-Driven Event Programming* later in this section for detailed procedures. Enter **0** to move to the "Access Sched?" prompt.
Access Sched. ? 1 = YES 0 = NO 0	Enter **1** to program access schedules. Refer to *Limitation of Access Schedules Programming* later in this section for detailed procedures. Enter **0** to move to the "Quit?" prompt.
Quit ? 1 = YES 0 = NO 0	Enter **1** to quit *#80 Scheduling Menu Mode* and return to normal operating mode. Enter **0** to make any changes or review the scheduling programming options. If you press **0**, the "Time Window?" prompt is displayed.

Time Windows

The system provides 20 time windows that are defined with start and stop times. These windows are used for various open/close and access schedules, as well as for output controls, and are the basis of the scheduling system. These windows are shared among all eight partitions.

Time Windows Worksheet

The following worksheet is an example of the worksheet found in the *Programming Guide*. This worksheet will help you define time windows and scheduling aspects of this system before you program them. Note that time windows **can** span midnight; for example, from 11 PM to 1 AM.

Time Window Number	Start Time (HH:MM)	Stop Time (HH:MM)
1		
2		
3.....20		

A time window must have a start and a stop time.

Time Windows Programming

Enter Scheduling Mode by entering **Installer Code + [#] + [80]**. The keypad displays the *Time Window Programming* prompt.

PROMPT	EXPLANATION
Time Window ? 1 = YES 0 = NO 0	Enter **1** at this main menu prompt to program time windows.
Time Window # ? 01-20, 00 = Quit 01	Enter the 2-digit time window number **(01-20)** to be programmed. Press [*] to accept the entry. Enter **00 + [*]** at the "Time Window #?" prompt to quit time window programming and display the "Quit ?" prompt.
01 TIME WINDOW 00:00AM 00:00AM	If you entered a time window number, the cursor is now positioned on the tens of hours digit of the start of window entry. Enter the desired start of window hour and press [*]. The cursor moves to the minutes position. Enter the desired minutes and press [*]. Toggle the AM/PM indication by pressing any key 0-9 while the cursor is under the A/P position and then press [*]. Repeat this to program the stop of window entry. When the entry is completed, the "Time Window #?" prompt is displayed again. Enter the next time window number to be programmed and repeat the procedure.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the Quit ? prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Because the time windows are shared among all partitions, it is important to make sure that changing a time window does not adversely affect desired actions in other partitions.

Daily Open/Close Schedules

Each partition can be assigned one daily open/close schedule, plus a holiday schedule. Temporary schedules are programmed separately, using the *#81 Temporary Schedule Menu Mode*. To program additional open/close schedules, see *Time-Driven Events Programming* later in this section for the procedure.

Open/Close Schedule Worksheet

The following worksheet is an example of the worksheet found in the *Programming Guide*. Write the previously defined time window numbers for open and close for each partition.

Part	Mon		Tues		Wed		Thur		Fri		Sat		Sun		Hol	
	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl
1																
2																
3...8																

Open/Close Schedule Programming

After entering Scheduling Menu Mode, press **[0]** until the "O/C Schedules?" prompt appears.

PROMPT	EXPLANATION
O/C Schedules ? 1 = YES 0 = NO 0	Enter **1** to program opening and closing schedules.
Partition # ? 01-08, 00 = Quit 01	Enter the appropriate partition number for which the following open/close schedules will apply. Enter **00 + [*]** at the "Partition #?" prompt to quit open/close schedules programming and display the "Quit ?" prompt.
Mon P1 OP WIND.? 00:00 00:00 00	Enter the time window number **01-20** for the displayed day's opening schedule beginning with Monday. Enter **00** if no schedule is desired for a particular day. As the number is keyed in, the actual time that has been stored for that window number is displayed as a programming aid. Press [*] to accept the entry.
Mon P1 CL WIND.? 00:00 00:00 00	Enter the time window number for the displayed day's closing schedule. As the number is keyed in, the actual time that has been stored for the window number is displayed. Press the [*] key to accept the entry.
Tue P1 OP WIND.? 00:00 00:00 00	The keypad now prompts for Tuesday's open/close schedule. Follow the procedure for Monday's prompts. When the last day of the week has been programmed, the holiday opening and closing window prompts are displayed.
Hol P1 OP WIND.? 00:00 00:00 00	Repeat the procedure for the holiday opening and closing time windows. Press the [*] key to accept the entry. When the entries are completed, the "Partition #?" prompt is displayed again. Repeat this procedure for each partition in the system.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the "Quit ?" prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Holiday Schedules

A holiday schedule overrides the regular daily open/close schedule on the programmed holidays throughout the year. The system provides up to 16 holidays that can be assigned for the system. Each holiday can be assigned to any combination of partitions but must always be assigned to Partition 1. List the desired holidays in a Month/Day format on the worksheet. Check the partitions for which these holidays apply.

Holiday Schedule Worksheet

The following worksheet is an example of the worksheet found in the *Programming Guide.*

HOL	Partition								
	Month/Day	1	2	3	4	5	6	7	8
1	/								
2	/								
3...16									

Holiday Schedule Programming

After entering Scheduling Menu Mode, press **[0]** until the "Holidays ?" prompt appears.

PROMPT	EXPLANATION
Holidays ? 1 = YES 0 = NO 0	Enter **1** to program holiday schedules.
HOLIDAY NUMBER ? 01-16,00=Quit 01	Enter the 2-digit holiday number **(01-16)** to be programmed and press [*] to accept entry. Enter **00 + [*]** at the "Holiday Number?" prompt to quit the holiday menus and display the "Quit ?" prompt.
01 ENTER DATE 00/00	The cursor is now positioned on the tens of months digit. Enter the appropriate month, then press [*] to proceed to the day field. Enter the appropriate day for the holiday. Press [*] to accept the entry.
Part ? 1 2 3 4 5 6 7 8 Hit 0-8 x x	Holidays can be set for any partition but must always include Partition 1, as follows. Press **[0]** to turn all partitions on or off, or use keys **1-8** to toggle the letter "x" under the partition to which this holiday will apply. Press the [*] key when all desired partitions have been assigned. The "Holiday Number?" prompt is displayed again. Repeat the procedure for each holiday to be programmed.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the "Quit ?" prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Time-Driven Events

These schedules are used to activate outputs, bypass zones, etc. based on time. There are 20 of these schedules that may be programmed for the system, each governed by the previously defined time windows.

The actions that can be programmed to automatically activate at set times are: relay commands, arm/disarm commands, zone bypassing commands, and open/close access conditions.

Time-Driven Events Worksheet

The following worksheet is an example of the worksheet found in the *Programming Guide*. Fill out the worksheet using the steps outlined below.

Schedule Num.	Time Window	Days								Action Desired	Action Specifier	Activation Time
		M	T	W	T	F	S	S	H			
1												
2												
3...20												

1. **Enter the schedule number (01-20) and time window number (01-20),** and note the day of the week the action is desired.
2. **Enter the code for the desired action and action specifier.** The action codes represent the events that are to take place when the scheduled time is reached. Each action also requires an action specifier, which defines what the action will affect (relay, relay group, partition, zone list, user group). The action specifier varies, depending on the type of action selected.

   The following is a list of the Action Codes (desired actions) used when programming Time-Driven events. Note that these codes are independent of the relay codes programmed during *Output Programming* in the *#93 Menu Mode*.

Relay Commands

Action Code	Action	Action Specifier
01	Relay On	Relay #
02	Relay Off	Relay #
03	Relay Close for 2 seconds	Relay #
04	Relay Close XX minutes (set in field 1*74)	Relay #
05	Relay Close YY seconds (set in field 1*75)	Relay #
06	Relay Group On	Relay Group #
07	Relay Group Off	Relay Group #
08	Relay Group Close for 2 seconds	Relay Group #
09	Relay Group Close XX minutes (set in field 1*74)	Relay Group #
10	Relay Group Close YY seconds (set in field 1*75)	Relay Group #

Arm/Disarm Commands

Action Code	Action	Action Specifier
20	Arm-STAY	Partition(s)
21	Arm AWAY	Partition(s)
22	Disarm	Partition(s)
23	Force Arm STAY (Auto-bypass faulted zns)	Partition(s)
24	Force Arm AWAY (Auto-bypass faulted zns)	Partition(s)
25	Arm INSTANT	Partition(s)
26	Arm MAXIMUM	Partition(s)

- The auto-arm warning (field 2*06) applies when using Time-Driven events to auto-arm.
- Temporary schedules do not override an auto-arming or auto-disarming programmed in Time-Driven events.
- The auto-arming window cannot be extended using the Installer Code + #82 Mode.
- Auto-arm and auto-disarm must not be disabled for the partition assigned in 2*05 and 2*07.

Bypass Commands

Action Code	Action	Action Specifier
30	Auto bypass – Zone list	Zone list #
31	Auto unbypass – Zone list	Zone list #

Open/Close Windows

Action Code	Action	Action Specifier
40	Enable Opening Window by partition	Partition(s)
41	Enable Closing Window by partition	Partition(s)
42	Enable Access Window for access group	Access Group

Access Control Commands

Action Code	Action	Action Specifier
55	Access Point Grant	Access Point #
56	Access Point Grant with Override	Access Point #
57	Access Point Protect	Access Point #
58	Access Point Bypass	Access Point #
59	Access Point Lock	Access Point #
60	Access Point Exit	Access Point #
61	Access Point Group Grant	Group #
62	Access Point Group Grant with Override	Group #
63	Access Point Group Protect	Group #
64	Access Point Group Bypass	Group #
65	Access Point Group Lock	Group #
66	Access Point Group Exit	Group #
67	Access Point Partition Grant	Partition #
68	Access Point Partition Grant with Override	Partition #
69	Access Point Protect by Partition	Partition #

Action Code	Action	Action Specifier
70	Access Point Bypass by Partition	Partition #
71	Access Point Lock by Partition	Partition #
72	Access Point Exit by Partition	Partition #
73	Access Point Trigger On	Trigger #
74	Access Point Trigger Off	Trigger #
77	Access Point Group Enable	Group #
78	Access Point Group Disable	Group #

3. **Enter the desired activation time** (when the action is to take place). Select from:

Activation Time	Description
1	Beginning of time window.
2	End of time window.
3	During time window active period only (on at beginning of window, off at end). For example, if bypass is selected to activate during the window, zones in a zone list are bypassed at the beginning of the window and unbypassed at the end of the window.
4	Beginning and end of time window (e.g., a coffee break buzzer). In this example, if relay pulse is selected, the relay pulses for 2 seconds at the beginning of the window, signaling the beginning of the coffee break. At the end of the window it pulses again, signaling the end of coffee break.
5	Random time at the start of the time window (occurs within 30 minutes after the start of the time window). **NOTE:** Since the randomization for choice "5" occurs within 30 minutes after the start of the window, the time window must be at least 30 minutes in duration.
6	Random time at the end of the time window (occurs within 30 minutes after the end of the time window).
7	Random during the time window (begins within 30 minutes after the start of the time window and ends within 30 minutes after the end of the time window). **NOTE:** Since the randomization for choice "7" occurs within 30 minutes after the start of the window, the time window must be at least 30 minutes in duration.

Field ∗04 must be enabled for randomization. A user must initiate a random schedule by entering one of the following sequences:

- **[User Code] + [#] + [41].** This will randomize, up to 30 minutes, the activation time of all devices, programmed for randomization, assigned to the partition the sequence is entered in. Enter the sequence again to turn off the random schedule.
- **[User Code] + [#] + [42].** This is the same as the method above, except the randomization occurs only on devices with activation times within 6 PM and 5 AM. Enter the same sequence again to turn off the random schedule.

UL You must not program Random Scheduling of Time Driven Events for UL installations.

Time-Driven Events Programming

The following menu items must first be programmed in *Output Programming in the #93 Menu Mode*:

Enter Relay No.	(reference identification number)
Output Group	(if applicable)
Restriction	
Output Type	(V-PLEX or 4204)
Zone No.	(V-PLEX)
ECP Address	(4204)
Relay No.	(4204)

After entering Scheduling Menu Mode, press **[0]** until the "Timed Events ?" prompt appears.

PROMPT	EXPLANATION
Timed Events ? 1 = YES 0 = NO 0	Enter **1** to program timed events.
TIMED EVENT # ? 01-20, 00=Quit 01	Enter the timed event number to be programmed **(01-20)**. Press [*]. The system then prompts the user to enter the desired action to be taken. Enter **00** at the "TIMED EVENT #?" prompt to quit the timed event menus and display the "Quit ?" prompt.
01 ACTION ? None 00	Enter the action code for this timed-event number from the list at the left. This could be an output command, an arming command, or any other Time-Driven event. Press [*] to accept the entry. The prompt for the action specifier appears.

ACTION CODES	EXPLANATION	ACTION SPECIFIER
01 = Relay On 02 = Relay Off 03 = Relay Close for 2 seconds 04 = Relay Close XX minutes 05 = Relay Close YY seconds	**Actions 01-05** If you selected actions **01-05**, the prompt at the right appears. Enter the relay number. Press [*] to accept entry. The "Time Window ?" prompt appears.	01 RELAY # ? 00
06 = Relay Group On 07 = Relay Group Off 08 = Relay Group Close for 2 seconds 09 = Relay Group Close XX minutes 10 = Relay Group Close YY seconds	**Actions 06-10** If you selected actions **06-10**, the prompt at the right appears. Enter the relay group number. Press [*] to accept entry. The "Time Window ?" prompt appears.	01 RELAY GRP # ? 00
20 = Arm-STAY 21 = Arm AWAY 22 = Disarm 23 = Force Arm STAY 24 = Force Arm AWAY 25 = Arm INSTANT 26 = Arm MAXIMUM 40 = Enable Open Window by Part. 41 = Enable Close Window by Part.	**Actions 21-26 and 40-41** If you selected actions **21-26** or **40-41**, the prompt at the right appears. Enter the partition to which the action applies. Enter **0** to select all partitions. Enter a partition number again to deselect it. Press [*] to accept entry. The "Time Window ?" prompt appears.	PART? 1 2 3 4 5 6 7 8 HIT 0-8 X X
30 = Auto bypass – Zone List 31 = Auto unbypass – Zone List	**Actions 30-31** If you selected actions **30-31**, the prompt at the right appears. Enter the zone list number that contains the zones to be bypassed or unbypassed. Press [*] to accept entry. The "Time Window ?" prompt appears.	01 ZONE LIST ? ENTER 01-15 01
42 = Enable Access Window for Access group(s)	**Action 42** If you selected action **42**, the prompt at the right appears. Enter the group number to which the time window will apply. Press [*] to accept entry. The "Time Window ?" prompt appears.	GROUP ?1 2 3 4 5 6 7 8 HIT 0-8 X
55 = Access Point Grant 56 = Access Point Grant w/Override 57 = Access Point Protect 58 = Access Point Bypass 59 = Access Point Lock 60 = Access Point Exit	**Actions 55-60** If you selected actions **55-60**, the prompt at the right appears. Enter the access point number. Press [*] to accept entry. The "Time Window ?" prompt appears.	01 ACCESS POINT # 000

PROMPT	EXPLANATION	ACTION SPECIFIER
61 = Access Point Group Grant 62 = Access Point Group Grant w/Override 63 = Access Point Group Protect 64 = Access Point Group Bypass 65 = Access Point Group Lock 66 = Access Point Group Exit 77 = Access Point Group Enable 78 = Access Point Group Disable	**Actions 61-66 and 77-78** If you selected actions **61-66**, the prompt at the right appears. Enter the group number. Press [*] to accept entry. The "Time Window ?" prompt appears.	GROUP # 00
67 = Access Point Partition Grant 68 = Access Point Partition Grant w/Override 69 = Access Point Protect by Partition 70 = Access Point Bypass by Partition 71 = Access Point Lock by Partition 72 = Access Point Exit by Partition	**Actions 67-72** If you selected actions **67-72**, the prompt at the right appears. Enter the partition to which the action applies. Enter **0** to select all partitions. Enter a partition number again to deselect it. Press [*] to accept entry. The "Time Window ?" prompt appears.	PART? 1 2 3 4 5 6 7 8 HIT 0-8 X X
73 = Access Point Trigger On 74 = Access Point Trigger Off	**Actions 73-74** If actions **73-74** were selected, the prompt at the right will be displayed. Enter the trigger number. Press [*] to accept entry. The "Time Window ?" prompt appears.	01 TRIGGER # 00

PROMPT	EXPLANATION
01 Time Window ? 00:00 00:00 01	Enter the time window number (**01-20**) for which this timed event is to occur. As the number is keyed in, the actual time that has been stored for the time window number is displayed. Press [*] to accept entry.
01 Active time ? 0	Enter the activation time from **1-10** (listed below). As the number is keyed in, the activation time is displayed. The choices are: **1:** Trigger at the start of the window. **2:** Trigger at the end of the window. **3:** Take effect only for the duration of the window. **4:** Trigger at both the start and the end of the window. Example: coffee break buzzer. **5:** Random trigger, up to 30 minutes, after the start of the window. **6:** Random trigger, up to 30 minutes, after the end of the window. **7:** Take effect only for the duration of the window, but random start and end the window up to 30 minutes. Press [*] to accept entry.
Days ? MTWTFSSH Hit 0-8 x x	The system then asks for which days the event is to be activated. Press **0** to toggle all days on or off; or press keys **1-8** to toggle the letter "x" under the day on or off (Monday = 1, Holiday = H = 8). When all entries have been made, the "TIMED EVENT #?" prompt is displayed again. Repeat the procedure for each timed event for the installation.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the "Quit ?" prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Bank Safe and Vault Example

The Bank Safe or Vault should be limited to its own partition where *only* a Master or Manager code would be allowed to operate 24-hours a day, whereas regular users can only operate between 6am and 10pm (see Section 2 of this Manual - Partitioning). To limit (disable) access to regular users to outside the desired time window follow the programming as shown below.

Desired Action

Panel will auto arm at 10pm Monday thru Saturday with no warning and Only Master/Manager can disarm between 10pm and 6am (they have 24 hour access).

#80 Programming

1. Enter Scheduling Mode by entering Installer Code + [#] + [80].
2. Select Time Windows, then enter the time below:

Window	*Start*	*Stop*	*Purpose*
1	6:00am	10:00pm	Monday-Saturday open window. (User must disarm within this window, otherwise control will disarm and send a "Late to Disarm" the appropriate report.)
2	9:30am	10:00pm	Monday-Saturday closing window (User must arm between 9:30pm and 10pm, otherwise the panel will arm and send a "Late to Arm" message.)

3. Enter 00 + * to exit Time Windows.
4. **Do not** Quit Menu Mode, go to O/C Schedules.
5. Enter the Vault Partition #.
6. Assign Window 01 as the OP window and Window 02 as the Cl Window for Monday thru Saturday.

Part	Mon		Tues		Wed		Thur		Fri		Sat		Sun		Hol	
	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl
1	01	04	01	04	01	04	01	04	01	04	01	04	00	00	00	00

7. Exit Program mode.

Control Programming

1. **2*05** = 00, Auto-Arm Delay (partition-specific) Arm at 10pm.
2. **2*06** = 00, Auto-Arm Warning Period (partition-specific) No Warning Period.
3. **2*07** = 00, Auto-Disarm Delay (partition-specific) Disarm at 6am.
4. **2*08** = 1, Force Arm (partition-specific) Enable.
5. **2*10** = 1, Allow Disarming only during Arm/Disarm Windows (partition-specific).
6. **2*11** = 0, Allow Disarm Outside Window if Alarm Occurs.

Disabling the Master/Manager Code

To also disable the Master/Manager from disarming between 10pm and 6am limits all Master/Manager codes access between 6am and 10pm Monday thru Saturday. They will not work on Sunday or Holidays.

1. Enter program mode Installers code + #80
2. Enter 'Time Windows' and Create window 03 for 6:00am-10:00pm, enter 00 + * to exit Time Windows
3. Do not Quit Menu Mode, go to Access Sched.
4. Create Access Sched 01 by assigning Window 03 to A1 Monday thru Saturday. Exit Program mode
5. Assign all Master and Manager Codes to Access Schedule 01 when user codes are assigned.

Removing the O/C schedule from Saturday

Open and Closed window can be removed from schedule for Saturday to prevent regular users (if they are enabled for this particular partition) from being able to disarm on Saturday, and window can be removed from Limit Access Group 1 for Saturday to prevent Master/Manager Access on Saturday.

1 Enter the program mode Installer's code + #80.
2. Go to O/C Schedules.
3. Enter Vault Partition, go to Saturday and enter 00 for OP and CL window.
4. Go to Access Schedules.
5. Enter Schedule 01, go to Saturday and enter 00 for Window A1. Exit program mode.

Holiday Schedules

Create selected Holidays in Holiday Programming and assign to all partitions. Holiday window in Open/Close Schedule remains empty to prevent regular users (if they are enabled for this particular partition) from being able to disarm on Holidays, and Limit Access Group 1 Holiday Window can remain empty to prevent Master/Manager Access on Holidays.

1. Enter program mode Installers code + #80.
2. Go to Holidays.
3. Enter Selected Holiday dates.
4. Exit program mode.

Limitation of Access Schedules

Limitation of Access is a means by which a user's access code is limited to working during a certain period of time. The system provides eight Access Schedules, each of which consists of two time windows for each day of the week and two time windows for holidays (typically, one for an opening time window and the second for a closing time window). A user, required to follow a schedule, would be assigned to an access group of the same number (e.g., schedule 1= group 1).

The user's access code is assigned to a group when that user is added to the system. If no limitations apply, enter **0**.

Limitation of Access Schedules Worksheet

Enter the appropriate time window numbers for each access schedule.

Acc	Mon		Tues		Wed		Thurs		Fri		Sat		Sun		Hol	
Sch	W1	W2	W1	W2	W1	W2	W1	W2	W1	W2	W1	W2	W1	W2	W1	W2
1																
2																
3...8																

NOTE: The holidays used for the access groups are the same as those defined in the holiday schedule.

Limitation of Access Schedules Programming

To program access schedules enter Scheduling Menu Mode **Installer Code + # 80**. After entering Scheduling Menu Mode, press **[0]** until the "Access Sched. ?" prompt appears.

PROMPT	EXPLANATION
Access Sched. ? 1 = YES 0 = NO 0	Enter **1** to program access schedules.
ACCESS SCHED # ? 01-08, 00 = Quit 01	Enter the access control schedule number between **01** and **08**. Press [*] to accept entry. Enter **00** at the "Access Sched #?" prompt to quit the access control menus and display the Quit ? prompt.
MON A1 Window 1? 00:00 00:00 00	Enter the first time-window number **(01-20)** for this access schedule for the displayed day. As the number is keyed in, the actual time that has been stored for the window is displayed. Press [*] to continue.
MON A1 Window 2 ? 00:00 00:00 00	Enter the second time-window number from **01-20** for this access schedule for the displayed day. As the number is keyed in, the actual time that has been stored for the window is displayed. Press [*] to continue.
TUE A1 Window 1? 00:00 00:00 00	Repeat the procedure for the other days of the week. When the last day of the week has been programmed, the windows for holidays may be entered.
Hol A1 Window 1 ? 00:00 00:00 00	Enter the first time-window number for holidays for this access schedule. As the number is keyed in, the actual time that has been stored for the window is displayed. Press [*] to continue.
Hol A1 Window 2 ? 00:00 00:00 00	Enter the second time-window number for holidays for this access schedule. As the number is keyed in, the actual time that has been stored for the window is displayed. Press [*] to continue.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the "Quit ?" prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Temporary Schedules

Each partition can be assigned a temporary schedule, which overrides the regular open/close schedule (and the holiday schedule). This schedule takes effect as soon as it is programmed, and remains active for up to one week.

Only users with the authority level of manager or higher can program temporary schedules.

A temporary schedule affects only the partition from which it is entered. Temporary schedules can also be reused at later dates simply by scrolling (pressing [#]) to the "DAYS?" prompt and activating the appropriate days. This should be considered when defining daily time windows.

Temporary Schedule Worksheet

Partition/Windows		Mon	Tue	Wed	Thu	Fri	Sat	Sun
1..8	**Disarm Window**							
	Start Time HH:MM							
	Stop Time HH:MM							
	Arm Window							
	Start Time HH:MM							
	Stop Time HH:MM							

Temporary Schedules Programming

Enter **User Code + [#] + 81** to enter this mode.

PROMPT	EXPLANATION
Mon DISARM WIND. 00:00AM 00:00AM	This prompt is for entering the start and end times of the disarm (opening) window for Monday. Upon entry of this mode, the cursor is positioned on the tens of hours digit of the start time of the disarm window. Enter the desired hour. Press [*] to move to the minutes field. The minutes are entered in the same manner. Press [*] to move to the AM/PM position. Pressing any key in the **0-9** range toggles the AM/PM indication. Repeat the procedure for the stop time entry. Press [*] to store the entries and move to the arming (closing) window for Monday. Pressing [#] scrolls you through the prompts without making any changes.
Mon ARM WINDOW 00:00AM 00:00AM	This prompt is for entering the start and end times of the arm (closing) window for Monday. The cursor is positioned on the tens of hours digit of the start time of the arm window. Enter the hour. Press [*] to move to the minutes field. The minutes are entered in the same manner. Press [*] to move to the AM/PM position. Pressing any key in the **0-9** range toggles the AM/PM indication. Repeat the procedure for the stop time entry. After the windows for that day have been completed, the system prompts for disarm and arm time windows for the next day. Press [#] if no changes are desired.
Tue DISARM WIND. 00:00AM 00:00AM	Repeat the procedure described above for all days of the week. When all the windows for all the days have been completed, the system prompts for which days of the schedule are to be activated.
Days ? MTWTFSS Hit 0-7 x x	This is the prompt that actually activates the temporary schedule. To select the days to be activated, enter **1-7** (Monday = 1). An "x" appears under that day, indicating the temporary schedule for that day is active. Entering a day's number again deactivates that day. Pressing **0** toggles all days on/off. The temporary schedule is in effect only for the days highlighted with the letter "x" under them. As the week progresses, the selected days are reset to the inactive state, but all other entries for the temporary schedule remain programmed. Press [*] to store the entries or press [#] to exit the Temporary Schedule Entry Mode without making any changes.

User Scheduling Menu Mode

The system provides up to 20 "timers" available to the end user to control output devices. The output devices themselves are programmed into the system by the installer during *Output Programming* in the *#93 Menu Mode*. The end user needs only to know the output device number and its alpha descriptor.

The installer may set certain outputs to be "restricted" during *Output Programming* (this prevents the end user from controlling doors, pumps, bell outputs, etc.)

To enter this mode, the user enters **User Code + [#] + 83.**

PROMPT	EXPLANATION
Output Timer # ? 01-20, 00=Quit 01	Enter the output timer number to be programmed **(01-20)**. Press [*] to accept entry and move to the next prompt. Enter **00** to quit and return to normal operating mode.
06 07:00P 11:45P PORCH LITE 04	If that timer number has already been programmed, a summary screen appears. In this example: 06 = Timer # 07:00PM = Start Time 11:45PM = Stop Time PORCH LITE = Descriptor for Output Device # 4 04 = Output Device # affected by this timer Press [*] to continue.
06 ENTER OUTPUT# PORCH LITE 04	Enter the desired output number **(01-96)**. As the number is entered, the descriptor for that output device is displayed. Press [*] to continue.

Entering **00** as the output number deletes the timer (Timer 06, in this example) and displays an output descriptor of "None." Output devices are programmed via #93 Menu Mode.

PROMPT	EXPLANATION
06 ON TIME ? 07:00 PM	The cursor is positioned on the tens of hours digit of the ON time. Enter the desired hour. Press [*] to move to the minutes field. The minutes are entered in the same manner. The AM/PM indication is toggled by hitting any key from **0-9** while the cursor is under the AM/PM position. Press [*] to continue.
06 OFF TIME ? 11:45 PM	The cursor positioned on the tens of hours digit of the OFF time. Enter the desired hour. Press [*] to move to the minutes field. The minutes are entered in the same manner. The AM/PM indication is toggled by hitting any key in the **0-9** range while the cursor is under the AM/PM position. Press [*] to continue.
06 DAYS? MTWTFSS HIT 0-7 x x	To select the days to be activated, enter **1-7** (Monday = 1). An "x" appears under that day, indicating the output for that day is active. Entering a day's number again deactivates that day. Pressing **0** toggles all days on/off. The outputs are in effect only for the days highlighted with the letter "x" under them. As the week progresses, the selected days are reset to the inactive state, unless the permanent option is selected (next screen prompt). When completed, press [*] to continue.
06 Permanent ? 0 = NO, 1 = YES 0	Selecting "Permanent" **(1)** means that this schedule will be in effect on a continuous basis. Selecting **0** means that this schedule will be in effect for one week only. The letter "x" under the day is then cleared, but all other entries for the output device remain programmed. Press [*] to accept entry. The system quits User Scheduling Mode and returns to normal operating mode.

Section 6: Software

(Remote Downloading is not a UL Listed feature)

General Information

Downloading allows the operator to remotely access, program, and control the security system over normal telephone lines, IP, or GSM Communicators. Anything that can be done directly from the keypad can be done remotely, using ADEMCO's COMPASS downloading software. To communicate with the control panel, the following is required:

System Requirements

System Attributes	Minimum	Recommended
Processor	Intel, Pentium II – 256 MB RAM Vista – 1GB RAM	Intel, Pentium, IV, 512 MB RAM (or above)
Disk Space (free)	1.5 GB	1.75 GB
Monitor Resolution	800 x 600	1024 x 768

Application	Version
Operating System	• Windows 2000 (SP4) • Window XP Professional (SP2 and SP3) • Window Vista 32-bit (Home, Ultimate & Business) • Compatible with the latest version of windows 7
Database Application	MS SQL Server
Microsoft Internet Explorer	5.5 and above

Phone Line Up Load/ Downloading Requirements

1. One of the following modems:
   - ADEMCO CIA and CIA2
   - Hayes Smartmodem 1200 (external: level 1.2 or higher; internal: level 1.1 or higher)
   - Hayes Optima 24 + Fax 96 external
   - Hayes Optima 336
   - BizComp Intellimodem 1200 w/volume
   - BizComp Intellimodem 2400

Other brands claim to be 100% compatible. These are not tested or supported.

Internal modems must have a 4-position DIP switch. Modems with a 6-position DIP switch will not work.

2. Compass revision 2.0 or above is required and can be found at https://mywebtech.honeywell.com/.

Getting On-Line with a Phone Line

At the protected premises, the control panel must be connected to the existing telephone line (refer to *SECTION 3: Installing the Control*). No programming of the panel is required before downloading to an initial installation.

When establishing a connection between the computer and the control panel, the following occurs:

Stage	What Happens
1.	The computer calls up the control panel. (The phone number for each customer must be entered into the customer's account file on the computer.)
2.	The control panel answers the phone call at the pre-programmed ring count and executes a handshake with the computer.
3.	The computer sends a request for callback to the control, unless callback is not required.
4.	The panel acknowledges the request and hangs up. During the next few seconds, the control processes the request, making sure certain encrypted information received from the computer matches its own memory.
5.	Upon a successful match, the control panel seizes the phone line and calls the computer back, unless callback is not required. (The phone number to which the computer's modem is connected must be programmed into the control field ∗35.)
6.	The computer answers, usually by the second ring, and executes a handshake with the panel.
7.	The panel then sends other default information to the computer. If this information matches the computer's information, a successful link is established. The system is now "on-line" with the computer.

- Alarms and Trouble responses and reports are disabled during actual uploading or downloading sessions. If you are on-line, but not actively uploading or downloading, all alarms report immediately. All other reports are delayed until you complete the session.
- The keypads remain active when on-line with a control, but are inactive during actual uploading or downloading sessions.

To download a control without programming any information, perform the following steps:

1. Enter the **Installer Code + [#] + [5]**. The panel temporarily enables a ring count of 5 and sets the Download Callback option to "1" (callback not required).
2. From the computer, call the panel using the downloader software set to "First Communication" Mode.
   The downloader establishes a session with no callback. The panel information can then be downloaded.

On-Line Control Functions

The following functions can be performed while on-line with a control panel (see field *37):

- Arm the system in the AWAY Mode; disarm the system
- Bypass a zone
- Force the system to accept a new program download
- Shut down communication (dialer) functions (for nonpayment of monitoring fees in an owned system)
- Shut down all security system functions (for nonpayment for a leased system)
- Inhibit local keypad programming (prevents takeover of your accounts)
- Leave a message for customer
  NOTE: Messages sent to the control panel from the downloader will be viewable at ALL partitions.
- Command the system to upload a copy of its resident program to the office
- Read: arming status, AC power status, list of faulted zones, list of bypassed zones, 1000 event log, list of zones currently in alarm, list of zones currently in trouble, and ECP equipment list
- Set the real-time clock

Telco Handoff

Telco handoff is another method of getting on-line with the downloader. The installer or customer enters the **User Code + [#] + [1]**, while on the phone line with the computer's modem phone line. The customer will get cut-off and the panel and download computer will establish a connection.

Access Security

The following four levels of protection guard the control against compromise while it is being accessed from a remote location:

1. **Security code handshake**
   The subscriber's account number as well as an 8-digit ID number (known only to the office) must be matched between the control and computer.
2. **Hang-up and callback**
   The control panel "hangs up" and calls the computer back at the pre-programmed number only if the security codes match (known as answering machine defeat).
3. **Data encryption**
   All data that is exchanged between the computer and control is encrypted to reduce the possibility of anyone "tapping" the line and corrupting data.
4. **Operator access levels**
   Operators may be assigned various levels of access to the downloader, each having its own log-on code. The access levels allow the operators read/write capabilities of the customers' account information. For a detailed explanation of the access levels, see the downloading software User Manual.

NOTES:

- Each time the control panel is accessed successfully, a Callback Requested report is sent to the central station, if Opening reports are programmed.
- When the system is downloading, the keypad displays "MODEM COMM."
- After each download (or Saved) an automatic time stamp is done, to indicate the last download (or save) and the operator ID number.
- A complete hard copy of each individual account can be obtained by connecting a printer to the computer. Refer to your computer Owner's Manual or contact your dealer for printer recommendations.

Downloading Using an AlarmNet Communicator

The control can be downloaded without using an approved AlarmNet communicator. For a list of compatible communicators visit MyWebTech. This can be accomplished using the ECP bus as explained in *Section 3 Installing the Control*.

Direct Connect Downloading

The control can be uploaded/downloaded on site via a direct connection. Below illustrates the proper wiring configuration for direct connect downloading.

NOTE: The direct-wire downloading connection is to be temporary, and is not part of the permanent installation.

Direct-wire downloading is meant as a tool for the installer during the installation process.

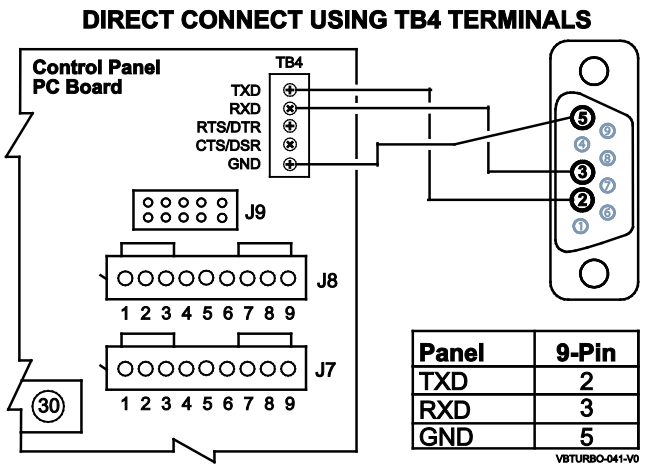


Figure 37: Direct Download TB4 Connections

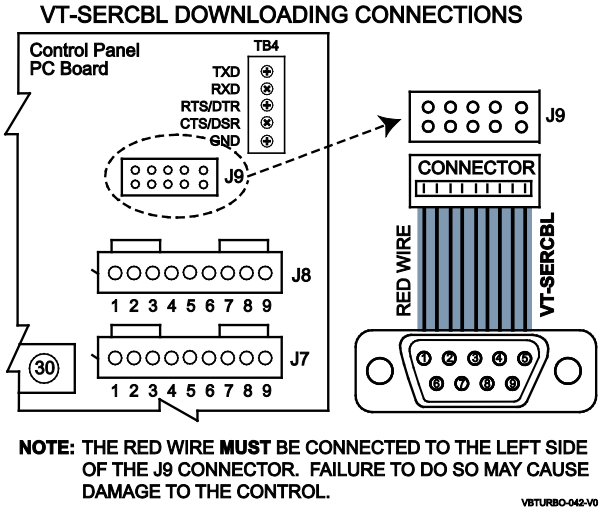


Figure 38: Direct Download VT-SERCBL Connections

To connect follow the instructions below:

1. Configure Compass for direct connecting (refer to *Compass Installation and Setup Guide* for more information.)
2. On an alpha keypad (non-touchscreen, such as a 6280 or Tuxedo Touch Wi-Fi) press **Installer Code + # + 5**.
3. Press connect on the Compass software.

   NOTE: For troubleshooting direct connecting issues, refer to https://mywebtech.honeywell.com/.

Section 7: System Clock

General Information

This system provides a real-time clock, which must be set in order for the system's event log to keep track of events by time and date. It must also be set in order to execute scheduling programs (Time-Driven events).

Only users with Installer or Master authority level can set the clock.

Setting the Time and Date

To set the real time clock, perform the following steps:

1. Enter Installer or Master Code + [**#**] **63**. Typical display shows:

TIME/DATE –– THU
12:01 AM 01/01/90

   The day of the week is automatically calculated based on the date entered. Time and date entries are made by simply entering the appropriate hour, minute, month, day and year.

   Press [*] to move the cursor to the right of the display, to the next position.

   Press [#] to move the cursor to the left of the display, to the previous position.

2. Enter the correct hour. Then press [*] to move to the "minutes" field.
3. Enter the correct minutes. Press [*] to move to the AM/PM position.
4. Press any key 0-9 to change AM to PM, or PM to AM. Press [*] to move cursor to the "month" field position.
5. Enter the correct month using a 2-digit entry. Press [*] to move cursor to the "day" field position.
6. Enter the correct day using a 2-digit entry. Press [*] to move cursor to the "year" field position.
7. Enter the correct year.

   Press [*] to exit the real-time clock edit mode.

Section 8: User Codes

General Information

The VISTA-128BPT allows a total of 150 security access codes to be allocated. The VISTA-250BPT allows a total of 250 security access codes to be allocated. Each security access code is identified by a user ID number. **Regardless of the number of partitions each code has access to, it occupies only one user slot in the system. If a code is not used in all partitions, that user ID number cannot be used again.**

The Quick Arm feature can also be programmed (partition-specific program field ∗29). The Quick Arm feature allows the user to arm the system by pressing the [#] key instead of the security code. The security code must always be entered to disarm the system.

A user code other than the installer code must be programmed in order for the Quick Arm feature to function.

The system is shipped with the following defaults for the user codes:

User	4-Digit Code	Alpha Descriptor
User 1 (Installer)	4140	INSTLR
User 2	1234	MASTER

User Codes & Levels of Authority

Each user of the system can be assigned a level of authority, which authorizes the user for certain system functions. A user can have different levels of authority within different partitions

Use the "View Capabilities" keypad function (**User Code + [∗] + [∗])** to view the partitions and authority levels for which a particular user is authorized. These levels are described below.

Level 0: Installer (User 1) Code

- Programmed in field ∗00 (default = 4-1-4-0). Installer Open/Close reporting selected in field ∗39.
- Can perform all system functions (arm, disarm, bypass, etc.), but **cannot disarm** if armed by another code (or by Quick Arm).
- Can add, delete, or change all other codes, and can select Open/Close reports for any user.
- Is the only code that can be used to enter program mode. The Installer Code can be prevented from re-entering the Program Mode by exiting using ∗98.
- Must program at least one Master Code during initial installation. Master Codes are codes intended for use by the primary user(s) of the system.

Level 1: Master Codes

- Can perform all normal system functions.
- Can be used to assign up to 148 lower-level codes, which can be used by other users of the system.
- Cannot assign anybody a level of 0 or 1.
- May change own code.
- Can add, delete, or change Manager or Operator Codes. Each user's code can be individually eliminated or changed at any time.
- Open/Close reporting is automatically the **same** as that of the Master who is adding the new user.

Level 2: Manager Codes

- Can perform all system functions (arm, disarm, bypass, etc.) programmed by Master.
- May add, delete, or change other users of the system below this level (Manager cannot assign anybody a level of 0, 1, or 2).
- May change own code.
- Open/Close reporting is automatically the **same** as that of the Manager who is adding the new user.

Levels 3-5: Operator Codes

- Can operate a partition, but cannot add or modify any user code (see table below).

Level	Title	Functions Permitted
3	Operator A	Arm, Disarm, Bypass
4	Operator B	Arm, Disarm
5	Operator C	Arm, Disarm only if armed with same code

- Operator C (sometimes known as the Babysitter Code) cannot disarm the system **unless** the system was armed with that code. This code is usually assigned to persons who may need to arm and disarm the system at specific times only (e.g., a babysitter needs to control the system only when babysitting).

Level 6: Duress Codes

- Sends a silent alarm to a central monitoring station if the user is being forced to disarm (or arm) the system under threat (system must be connected to a central station).
- Assigned on a partition-by-partition basis, and can be any code or codes desired.

Duress Reporting **NOTE:** A non-zero report code for zone 992 (duress) must be programmed, and partition-specific field *85 duress location enabled, to enable Duress reporting.

- The Duress report-triggering logic activates on the 5th key depression (such as OFF), not the 4th key depression (last digit of code). Duress reports are not triggered if the 5th key is a [*], such as when you perform a GOTO or view the capabilities of a user.

General Rules on Authority Levels and Changes

The following rules apply to users when making modifications within the system based on the user code authority levels:

- Master Codes and all lower-level codes can be used interchangeably when performing system functions within a partition (a system armed with a user's temporary code can be disarmed with the Master Code or another user's temporary code), except the Operator Level C Code described above.
- A user may not delete or change the user code of the SAME or HIGHER authority than that which he is assigned.
- A user (levels 0, 1 and 2 only) may only ADD users to a LOWER authority level.
- A user may assign other users access to only those partitions to which he himself has access.
- A user code can be DELETED or CHANGED only from within the partition it was created in.
- User numbers must be entered in 3 digits. Single-digit user numbers must, therefore, always be preceded by a "00" (e.g., 003, 004, 005, etc.). Make sure the end user understands this requirement. Temporary codes are entered as 4-digit numbers.

Open/Close Reporting Note:

When a user is added, the system prompts for Open/Close reporting capability **only** if the installer is adding the new user. When a Master or Manager adds a new user, the new user's Open/Close reporting is the same as that of the Master or Manager who is adding the user. If Open/Close reports are required to be selectable by the Master or Manager, the Installer should assign two Master or Manager user codes: one with Open/Close reporting enabled, and one without.

Note that Open/Close reporting of Quick Arm is enabled if User 002 is enabled for Open/Close reporting, and that Quick Arm reports as User 000. In order for Quick Arm reports to be sent for all partitions, User 002 must have authority and Open/Close must be enabled for all partitions. If a code with access to all partitions is not desired, it is suggested that user 002 be assigned authority level 5 in all partitions, and that the code be kept secret. Authority level 5 cannot disarm the system unless armed by that user.

ADEMCO Contact ID format is capable of reporting Users 001-150 uniquely. If any other report format is used, only user numbers 001 – 015 can uniquely report to the central station. Users 016 – 150 will report as User 015.

Multiple Partition Access

Each user is programmed for a primary (home) partition. A user can also be given access to operate one or more additional partitions. Within each partition, each user may be programmed to have different levels of authority. For example, User 003, the VP of Engineering, could be assigned to work within the Engineering Department (Partition 1) of ABC Manufacturing. Because he needs the full capabilities in his area, he is assigned as a MASTER with Level 1 authority.

He must also be able to gain access to the manufacturing area (Partition 2) on an emergency basis. You can set this up easily by requesting that he also be assigned to Partition 2, with a level of authority set lower, such as Level 4 (OPERATOR Level B).

The control automatically assigns him the same user number within Partition 2.

EXAMPLE OF MULTIPLE PARTITION ACCESS

Part 1	Part 2	Part 3	Part 4	Part 5	Part 6	Part 7	Part 8
User 3	User 3						
Level 1	Level 4						
Master	Oper B						

In the above example, User 3 has MASTER authority in Partition 1 and OPERATOR B authority in Partition 2. His user number is the same for both partitions. Note that if a user number is already being used in a partition, the system will automatically assign a new user an unused number. Also notice that no access is allowed for this user into Partitions 3 – 8. Attempts to access these partitions would be denied automatically.

Adding a Master, Manager, or Operator Code

During user code entry, normal key depressions at other keypads in a partition are ignored. However, panic key depression causes an alarm and terminates user entry.

Enter **Installer Code + [8] + new user no. (002-250) + new user's code**

†Or Master or Manager Code, but the code must be a higher level of authority than the code being changed (e.g., a Manager Code can add an Operator-level Code, but cannot add a Master or another Manager Code). Keypad prompts for the authority level for this user.

NOTE: All references to the number of user codes pertain to the VISTA-250BPT. The VISTA-128BPT allows only 150 user codes.

PROMPT	EXPLANATION
User Number = 003 Enter Auth. Level	Enter the level number as follows: 1 = Master 2 = Manager 3 = Operator Level A 4 = Operator Level B 5 = Operator Level C 6 = Duress Keypad then prompts for Open/Close reporting option for this user.
Open/Close Rep.? 0 = NO , 1 = YES	Press **0** (NO) or **1** (YES), depending on whether or not arming/disarming by this user will trigger Opening and Closing reports. This prompt appears only if the Installer Code is used to add a user.
Group Bypassing? 0 = NO , 1 = YES	Enter 1 (YES) to allow this user to perform group bypasses. Enter 0 (NO) this user will not be able to perform group bypasses. **NOTE:** In addition to enabling the user for group bypassing, the user **must also have access to the partition(s) containing the zones being bypassed and have global arming capability**.
Access Group? Enter 0-8	If access schedules have been programmed, this prompt appears. Enter the user's access group number (1-8) if this user should have limited access to the system. Enter **0** if no access group should be assigned.
RF Button ? 0=NO , 1=YES	If a 5800 Series button transmitter has been enabled for arming/disarming functions, and is not assigned to a user, this prompt appears. Press **0** (NO) or **1** (YES).
Enter Button ZN # (001-087)	If you answered "yes" to the RF button question, the zone number for the button is requested. Enter any one of the zone numbers assigned to the button transmitter as AWAY, STAY, or DISARM. The system then assigns **all** buttons of the transmitter to this user number.

PROMPT	EXPLANATION
Multi-Access ? 0 = NO , 1 = YES	Press **0** (NO) if the user is to have access to this partition only. Press **1** (YES) if the user is to have access to more than one partition. If NO, the program exits this mode. If YES, the keypad prompts for the Global Arm option for this user.
Global Arm ? 0 = NO , 1 = YES	Press **0** (NO) or **1** (YES), depending on whether this user will be allowed to arm more than one partition via Global Arm prompts. The keypad now prompts for the user's access to the next partition.
Part. 2 – SHOP ? 0 = NO , 1 = YES	Press **0** (NO) or **1** (YES), depending on whether this user will have access to the displayed partition number. If NO, the keypad displays this prompt for the next partition number in sequence. If YES, the keypad prompts for the following: • User's authority level in the displayed partition (see Authority Level prompt above). • Open/Close option for this user in the displayed partition (see Open/Close prompt above). • Global Arm option for this user in the displayed partition.
NOTE: When all partitions have been displayed, the keypad will scroll through all partitions to which access has been assigned, and will display the user number, authority level, open/close and global arm options that were programmed for each partition to which the user was granted access.	
Part. 1 A0* WHSE User 003 Auth=3G.	Note that the "G" following the authority level indicates that the global arm feature is enabled for this user in the displayed partition, and that the period at the end of the second line indicates Open/Close reporting is enabled for this user in the displayed partition. The [*] indicates the partition from which the user may be changed or deleted.

Changing a Master, Manager, or Operator Code

Enter **Installer Code*+ [8] + new user no. (002-250) + new user's code**

*Or Master or Manager Code, but the code must be a higher level of authority than the code being changed (e.g. a Manager Code can add an Operator-level Code, but cannot add a Master or another Manager Code).

NOTE: The VISTA-128BPT allows only 150 user codes.

PROMPT	EXPLANATION
User Number = 003 ADD NEW USER?	The system detects that the user number is already assigned, and prompts if this is a new user. Press **0** (NO). The system then confirms that the change is allowed based on authorization level.

Adding an RF Key to an Existing User

To add an RF key to an existing user, or to change a user's global arm option, first delete that user's code, then re-add the user code as described in the "Adding a Master, Manager, or Operator Code" paragraph.

Deleting a Master, Manager, or Operator Code

Enter **your code*+ [8] + new user no. (002-150) + your code again**

*Or Master or Manager Code, but the code must be a higher level of authority than the code being changed (e.g. a Manager Code can add an Operator-level Code, but cannot add a Master or another Manager Code).

NOTE: The VISTA-128BPT allows only 150 user codes.

PROMPT	EXPLANATION
OK TO DELETE 003? 0=NO 1=YES	The system prompts to confirm that you want to delete this user. Press **0** (NO) or **1** (YES). If you answered "yes," that user's code is removed from all partitions to which it was assigned, and all authorization levels and other information about that user are deleted. Note that a user can be deleted only by a user with a higher authority level. A user cannot delete himself.

A user code can be deleted only from the partition through which it was entered. If an attempt is made to delete from another partition, the message "User [XXX] Not Deleted" is displayed.

Exiting the User Edit Mode

Press either [*] or [#], or don't press any key for 10 seconds.

Section 9: Testing

Battery Test

When AC power is present, the VISTA-128BPT/VISTA-250BPT runs a brief battery test every 60 seconds to determine if there is a battery connected, and runs an extended battery test every 4 hours to check on the battery's condition.

If the VISTA-128BPT/VISTA-250BPT finds that the battery voltage is low (less than approximately 11.5V), it initiates a keypad "SYSTEM LOBAT" display and a rapid keypad beeping sound. It also sends a Low Battery report to the central station (if programmed). **The keypad is cleared by entering any security code + OFF**, and a Restore report is sent to the central station if the situation has been corrected.

Test Reporting

The VISTA-128BPT/VISTA-250BPT may be programmed to automatically transmit test reports to a central station at intervals ranging from once per hour to once per 9999 hours (field *27).

UL requires the test report to be transmitted at least once every 24 hours. The system can be programmed to send the first report at any time of the day, or on any day of the week (field *83).

Burglary Walk-Test (Code + [5] TEST)

NOTES:

- Test mode is active only for the partition at which test mode is entered. Other partitions are still operative and will cause the external sounder and communicator to activate if an alarm condition occurs.
- The control enters test mode if there are zones faulted, but will not go into test mode if zones are bypassed or in trouble.

This test causes the system to sound keypad beeps in response to faults on zones for the purpose of allowing proper zone operation to be checked without triggering alarms. **This test can be activated by an Installer, Master, or Manager User code by entering the corresponding security code and pressing TEST** while the burglary portion of the system is disarmed. UL requires that this test be conducted on a weekly basis.

- When this test is first entered, the system activates the alarm output (siren) for 3 seconds.

  NOTE: If the sounder does not sound, this may be an indication that the backup battery is discharged or missing, and should be showing a low battery on the keypad.

  It will also clear a low battery if the voltage is above 11.5VDC
- The system sends a Start of Walk-Test message to the central station (if programmed in *93, report codes, system group 4).
- The keypad displays "Burg Walk Test in Progress" and sounds a single beep every 15 seconds while the test remains active.

Open and close each protected door and window in turn. Each action should produce three beeps from the keypad. Walk in front of any motion detectors. Listen for three beeps when the detector senses movement.

See "Go/No Go Test Mode" for instruction on testing wireless transmitters.

The keypad displays the zone number and alpha descriptor while a door or window remains open or while a detector remains activated.

To end this test, enter any security code and press OFF. An End of Walk-Test message is sent to the central station.

The system automatically exits the Test mode if there is no activity (no doors or windows are opened and closed, no motion detectors are activated, etc.) for 30 minutes on the VISTA-128BPT, 60 minutes on the VISTA-250BPT. The system beeps the keypad(s) twice every 15 seconds during the last 5 minutes as a warning that it is about to exit the Test mode and return to normal operation.

Testing Wireless Transmitters

Transmitter ID Sniffer Mode

Use the Transmitter Sniffer Mode to test that transmitters have all been properly programmed. (This test can be used to verify the number of wireless zones programmed.)

If a transmitter does not have its serial number "enrolled," it will not turn off its zone number.

To enter the Transmitter ID Sniffer Mode, proceed as follows:

1. Enter **Installer Code + [#] + [3].** The keypad displays all zone numbers of wireless units programmed into the system.
2. Fault each wireless zone, causing each device to transmit.
   As the system receives a signal from each of the transmitters, the zone number of that transmitter disappears from the display.
3. Enter **Installer Code + OFF** to exit the Sniffer Mode.

Go/No Go Test Mode

Checking the transmitters in this mode assists in determining good mounting locations, and verifies that the RF transmission has sufficient signal amplitude margin for the installed system.

- All partitions containing wireless transmitters must be placed in the test mode for sensitivity reduction of the RF receiver (50% sensitivity). Otherwise, the RF receiver remains at full strength.
- Make sure that all partitions are disarmed when performing this test, as the wireless receiver gain is reduced in half.
- When panel is in Test mode wireless keys will not arm or disarm system. When button is pressed it will show a fault of the zone assigned to wireless key. Fault will not clear until taken out of Test mode.

1. Enter **Installer Code + [5]**.
2. Fault each wireless transmitter, causing each device to transmit.
   NOTES:
   - If a single receiver is used, the keypad beeps three times to indicate signal reception.
   - If two receivers are used, the keypad beeps once if the first receiver received the signal, twice if the second receiver received the signal.
   - It will beep three times if both receivers heard the signal.
3. If the keypad does not beep, reorient or move the transmitter to another location. Usually a few inches in either direction is all that is required.
4. Enter **Installer Code + OFF** to exit the Go/No Go Test Mode.

Armed Burglary System Test

Alarm messages are sent to the central station during the armed system tests. Notify the central station that a test will be in progress.

A display of "COMM. FAILURE" indicates a failure to communicate (no kissoff by the receiver at the central station after the maximum number of transmission attempts is tried). If this occurs, verify that the phone line is connected, the correct report format is programmed, etc.

1. Notify the central station that a test of the system is being performed.
2. Arm the system.
3. Fault one or more zones.
4. **Silence alarm sounder(s) each time by entering the code and pressing OFF.**
   NOTE: The system must be rearmed after each code + off sequence.
5. Check that entry/exit delay zones provide the assigned delay times.
6. Check the keypad-initiated alarms, if programmed, by pressing the panic key pairs (* and #, 1 and*, and/or 3 and #).
   The word ALARM and a descriptor "999" are displayed for * and #. If [1] and [*] are pressed, "995" is displayed; if [3] and [#] are pressed, "996" is displayed.
7. If the system has been programmed for audible emergency, the keypad emits a loud, steady alarm sound. Silence the alarm by entering the security code and pressing OFF. If the system has been programmed for silent panic, there are no audible alarms or displays. A report is sent to the central station, however.
8. Notify the central station that all tests are finished, and verify results with them.

Smoke Detector Test

All smoke detectors must be tested monthly by pressing the TEST button located on the detector. If the TEST button does not cause the detector to activate it must be replaced immediately.

Trouble Conditions

Check or Trouble Messages

Display	Description
CHECK or TRBL **(as per field 1∗07)**	This indicates that a problem exists on the zone number displayed. Zone trouble may be caused by one of the following conditions: • A hardwired fire zone is open (broken wire). • A zone programmed for tamper on Open/Short has been tampered. • A Day/Night zone (zone type 5) is faulted. • A polling loop zone is not seen by the control panel. • A polling loop zone has been tampered (cover removed on a V-PLEX device). • A wireless zone has not checked in during the time programmed in field 1∗31. • A 5800 Series transmitter has been tampered (cover removed).
CHECK 8XX **XX = 00-30**	This indicates a trouble on a peripheral device (connected to the panel's keypad terminals) of the corresponding device address (00-30).
CHECK 9XX **XX = 00-99**	This indicates that a system trouble exists (RF receiver, bell output, etc.).

If the problem has been corrected, enter an OFF sequence (**Security Code + OFF**) twice to clear the display.

Power Failure

Display	Description
AC LOSS **POWER LED is off**	This indicates that the system is operating on battery power only. Check to see that the circuit breaker for the branch circuit that your system's transformer is wired to has not been accidentally turned off. **Instruct the user to call a service representative immediately if AC power cannot be restored.**

Other System Messages

Display	Description
COMM FAILURE	This indicates that a failure occurred in the telephone communication portion of your system.
LO BAT	This indicates that a low-battery condition exists in the wireless transmitter displayed. Pressing any key silences the audible warning sound.
SYSTEM LO BAT	This indicates that a low-battery condition exists with the system's backup battery.
RCVR SETUP ERROR	This indicates that the system has more wireless zones programmed than the wireless receiver can support. If this is not corrected, none of the zones in the system will be protected. If additional wireless zones are desired, use an appropriate receiver.
MODEM COMM	This indicates that the control is on-line with a remote computer.

To the Installer

Regular maintenance and inspection (at least annually) by the installer and frequent testing by the user are vital to continuous satisfactory operation of any alarm system.

The installer should assume the responsibility of developing and offering a regular maintenance program to the user as well as acquainting the user with the proper operation and limitations of the alarm system and its component parts. Recommendations must be included for a specific program of frequent testing (at least weekly) to ensure the system's proper operation at all times.

Turning the System over to the User

Fully explain the operation of the system to the user by going over each of its functions, as well as the User Guide supplied.

In particular, explain the operation of each zone (entry/exit, perimeter, interior, fire, etc.). Be sure the user understands how to operate any emergency feature(s) programmed into the system.

Contacting Technical Support

PLEASE, before you call Technical Support, be sure you:

- READ THE INSTRUCTIONS!
- Check all wiring connections.
- Determine that the power supply and/or backup battery are supplying proper voltages.
- Verify your programming information where applicable.
- Verify that all keypads and devices are addressed properly.
- Note the proper model number of this product, and the version level (if known) along with any documentation that came with the product.
- Note your Honeywell customer number and/or company name.

  Having this information handy will make it easier for us to serve you quickly and effectively.

Technical Support:	1-800-323-4576 (8 a.m.-8 p.m. EST)
MyWebTech:	https://mywebtech.honeywell.com/

Section 10: Glossary

A

- **AAV:** Abbreviation for Audio Alarm Verification (*see also Two-way)
- **Access Code:** user code (a.k.a. security code); required to perform all security system functions
- **Access Control Relay:** This relay is used to control an electronic door strike via a simple keypad command
- **Access Schedules:** In some controls users may be assigned to 1 or more access schedules which limit the times these users may arm and disarm the system
- **Address; Addressable:** Devices such as keypad, wireless receivers, and relay modules must be addressed (00-31), usually through dip switch settings, or in the programming of the device
- **ADEMCO Contact ID:** Allows an alarm to be reported to the central station in about 3 seconds.
- **ADEMCO High Speed:** Allows an alarm to be reported to the central station in about 3 seconds.
- **Alpha Keypad:** Allows the use of English Language Display; used for programming and anything with descriptors
- **Alpha Descriptor:** An English Language name or description of a zone, Such as "Jane's Bedroom Window", as apposed to just "Zone 2"
- **Alpha Numeric:** The use of the alphabet and numbers
- **Arm:** To turn the security system On (*see also, Away mode, Stay mode, Instant mode, and Maximum mode)
- **Auto-Arm:** On supported control the system can be set up to automatically arm at a certain time.
- **Auto-Disarm:** * See Auto-Arm
- **AUI:** Advanced User Interface; our touch screen keypads 6272 and 6280 series
- **Aux.:** The abbreviation for auxiliary, i.e. Aux Power
- **Auxiliary Power Output:** Each Vista Control provides a Limited amount of power for peripheral devices such as a 4-wire smoke and Motion Detectors, etc.
- **Away Mode:** All Vista Control Panels have the ability to arm Away. This mode arms all perimeter and interior zones.
- **AWG:** Average Wire Gauge; the standard by which wire is measured; wire thickness in millimeters. Standard in the alarm industry is 22awg.

B

- **Backlighting:** Refers to the lighting up of the keypad's keys and/or display screen
- **Battery Calculations:** To meet certain UL regulations the system battery must have the capacity to power the system during an AC loss for xx hours; The Fire Control panels have battery calculations charts that help the installer determine the necessary battery size.
- **Bypass:** To temporarily disable 1 or more zones

C

- **CPU:** Computer processing unit; main pc board
- **C.S.F.M:** California State Fire Marshal; agency listing for fire controls in California (a.k.a. CFM)
- **Check:** When displayed, indicates that a trouble condition exists
- **Chime** (Chime Mode): When enabled, with the system turned off, the keypad will beep 3 times whenever a door or window opens up. They must be programmed for a Zone Type of 01, 02, 03, 24 and configurable (panel dependant)
- **CID:** Abbreviation for Contact ID
- **Code:** *see also report code, access code
- **Common Lobby:** Some partitioned controls provide for a partition to be a "common" partition which employs logic for automatic arming and disarming of the common lobby (ie; Dr.'s office, etc.).
- **Console:** Keypad (a.k.a. touch pad or control pad)
- **Contact ID:** *See ADEMCO Contact ID
- **Control Board:** The main PC Board (a.k.a. the panel; control; PCB; or CPU)
- **Control Software (or firmware):** The micro-chip that contains the actual program code that runs the control panel (a.k.a. prom chip)
- **Custom Words:** Controls that support programmable alpha have a built-in Dictionary list, if the word is not in the list they can create that word as a custom alpha descriptor.

D

- **Daily Schedule:** A partition can have a daily schedule created. This schedule is generally used to determine when the system will Auto Arm and/or Disarm, but it can also be used for special reporting purposes.
- **Default Screen:** On Alpha Keypads, when the system is disarm the default message is "Disarmed . . . Ready to Arm". On some controls, this default screen can be changed by the installer to say anything up to 32 characters.
- **Direct-Downloading:** (*see also download) Allows the installer to connect directly to the control panel on site via a laptop without a phone line.
- **Disarm:** To turn the system OFF
- **Download:** To send the program data or commands in the Computer to the control panel
- **Download ID Number:** A user-changeable 8-digit number that is downloaded to the control panel on the initial connection, and must match on any future connection.
- **D.T.M.F.:** Abbreviation for Dual Tone Multi-Frequency, or Touch Tone
- **Dual Reporting:** When the same report goes to two separate central station or receivers

E

- **ECP:** Abbreviation for Enhanced Console Protocol; This is the way that devices such as addressable keypads, wireless receiver and relay modules "talk" to the control panel on the keypad buss.
- **EOLR:** Abbreviation for End of Line Resistor used on Zones
- **EOLSR:** Abbreviation for End of Line Supervision Relay used on 4-wire smoke detector zones.
- **Earth Ground:** All control panels provide an Earth Ground terminal to wire to a ground post. This ground connection can be used to ensure protection against lightning hits and power surges; as a reference point for supervising telephone lines and zone wiring ground fault detection
- **Encryption:** Encoding; Encryption is used in the Compass Downloading Software to encode account files. Also used in wireless to prevent code stealing
- **End of Line Supervision Relay:** Relay used to supervise the power on 4-wire smoke detectors
- **Event Log:** In some controls events can be stored for later viewing; *Events; Event Log Types.
- **Events:** Situations that have occurred, i.e. Alarms, Troubles, Arming, Disarming, etc.
- **Event Log Types:** The event log stores events in many categories such as: Alarms, Checks (troubles), Bypasses, Open/Close (Disarm/Arm) System (loss of ac, battery, etc.), and Test
- **Exit Error Alarm:** An alarm caused by leaving an entry/exit door open after arming.
- **Expansion Module:** On some controls additional modules may be used to add zones. May be a wireless, Multiplex (polling loop), or Hardwire Zone module.
- **Expansion Zones:** Zones that are added to the system; May be wireless, Multiplex, or Hardwire Zones.

F

- **F.M.:** Factory Mutual; Agency listing for commercial fire controls nation-wide
- **Factory Default:** All controls come from the factory with a set of default values for each option; these defaults are the most popular choices for each available options; Factory defaults can be loaded at anytime by hitting *97 in the panels program mode.
- **Fixed Word:** All Honeywell keypads use English language displays; some keypads ("alpha") are capable of fully programmable alpha-numeric description for each zone; other keypads are non-alpha programmable but uses Fixed Glass words on the display, such as Ready, Not ready, Armed, Disarmed, etc.
- **Forced Bypass:** To automatically bypass all open zones at once.

G

- **Global-Arm/Disarm:** In a multi-partitioned system users that have access to more than one partition may have the option to arm/disarm all of their accessible partitions at the same time.
- **Go/No Go Test:** This is a patented test (for wireless systems) that gives the installer a definitive Yes or No as to the placement of wireless transmitters.
- **GoTo:** In a partitioned system the GoTo command allows users, with access to more than 1 partition, to log on and control one partition from another partition's keypad
- **GUI:** Graphic User Interface

H

- **Hardwire Expansion:** The ability to add additional hardwire zones to some controls by adding a hardwire expansion module
- **Heat Detector (Heat Stat):** A device that activates when the ambient temperature reaches 135 degrees (or 190); other types measure quick rises in temperature ("rate of rise")
- **Holiday Schedule:** A Holiday Schedule overrides the regular daily schedule on selected holidays throughout the year.
- **Horn:** An indoor sounder generally used in fire systems
- **Horn-Strobe:** An indoor sounder with a built in strobe light used in fire systems
- **House ID:** In a 5800 Series wireless system a 2-digit house ID can be used for feedback status for wireless keys, wireless keypads, etc.

I

- **Installer Code:** The 4 digit code that allows the installer to enter the Panels programming mode; the installer code can not be used to disarm unless it was used to arm.
- **Instant Mode:** One of the arming modes; when armed Instant all perimeter protection is on; all interior protection is off; there is exit delay time but NO entry delay time.

J

- **Junction Box:** A box or splice point where wires come together or branch off in an installation

K

- **Keypad: a.k.a.** Console, Touchpad, Control pad; Used to control all system functions and programming
- **Keyswitch:** A device used to arm and disarm the system using a hard key

L

- **LCD:** Liquid Crystal Display
- **LED:** Light Emitting Diode
- **Learn Mode:** The learn mode allows 5800 Series wireless transmitters or V-PLEX® Serial Poll devices to be programmed into the system simply by tripping the device. (i.e. door or window); The 5800 series transmitters and V-PLEX® Serial Poll devices send unique serial numbers that are learned for that zone
- **Limited Access:** Some controls may be programmed to allow certain codes to only work during certain times. (*see also Access schedules)
- **Line Fault:** Term used to describe the loss of telephone line voltage
- **Line Fault Monitor, LFM:** A device used to supervise the telephone line voltage at the control panel and to alert when the line is cut. ie: 659en

M

- **M.E.A.:** Material Evaluation Authority; agency listing for commercial fire installations in Manhattan, New York
- **Master Console:** Some partitioned controls allow keypads to be designated as a "master" which displays the status of all partitions at once.
- **Maximum Mode:** One of the arming modes; when armed maximum all perimeter and interior zones are protected with no entry delay (when initially arming you will have an exit delay).
- **Multiplex Loop:** a.k.a. polling loop, V-PLEX®; some controls can support multiplex expansion devices such as PIRs, smokes, 8 zone expanders, etc.

N

- **NBFAA –** National Burglar and Fire Alarm Association; a national association comprised of security and fire industry professionals; provide training for people in the security/fire industry;
- **NFPA:** National Fire Prevention Association: a national association that sets forth standards for fire system installations
- **Night-Stay Arming:** arming the system in the stay mode, however (depending on the panel) you can choose which interior zones will not be bypassed.

O

- **Open/close by user:** Primarily in commercial application open/close (arm/disarm) reports along with the user number may be sent to the central station; also logged by the event log in some controls
- **Output Timers:** Some controls may be programmed to automatically control relays, lights, and appliances on a timed basis; these outputs, in some cases, may also be controlled from the keypad as well.

P

- **PIR:** Abbreviation for Passive Infrared motion detector
- **Partition:** An area within a total system that can be separately controlled as if it were an individual system.
- **Partition Descriptor:** A 4-character name that can be programmed in some controls to identify each partition.
- **Partition Specific:** A feature option that relates directly to a partition as opposed to the system as a whole
- **Periodic Test Report:** A report sent to central station on a regular basis; Programmable in some controls, but usually happens every 24 hours; UL requirements in commercial applications; Used to verify the dialer is still working properly even though it has not sent any reports
- **Phone access:** The ability to access and control the security system via touch tone phone on or off premise
- **Phone Code:** A 2-digit code required to access the security system via touch tone phone.
- **Polling loop:** A 2-wire loop used to support multiplex devices on some controls; *see also multiplex Loop and V-PLEX®
- **Program Field:** A specific address in programming
- **Program Mode: T**he mode through which the installer programs the security system from the keypad
- **Pull Station:** A device that allows a manual initiation of a fire alarm, such as the 5140MPS

Q

- **Quick-Arm:** The option to use the [#] key in place of the 4-digit code when turn the system on (arming); Can be used to arm away, stay, instant, and maximum. The 4-digit code is required to disarm the system.
- **Quick Bypass:** Some controls have the option to bypass all faulted zones by pressing the [Bypass] key + [#] key at the keypad.

R

- **Real Time Clock (RTC):** a built-in clock that keeps real time, for test reports, scheduling, and output timers; the time and date may be set via the keypad
- **Relay:** A mechanical device or switch used to transfer power, or to create an open or short in a circuit
- **Relay Module:** An addressable module used on some controls; 4204, 4229, or 4101SN
- **Relay Output:** Some controls support programmable Relay Outputs; these can be 4204, 4229, or 4101SN
- **Report Code:** The alpha-numeric report that is transmitted to the central station receiver to identify the events that have occurred
- **Report Format:** The Language in which an alarm report is set to the central station
- **Restricted Output:** Relay Outputs may be restricted to from end-user control
- **RF:** Abbreviation for Radio Frequency, wireless
- **RTC:** Abbreviation for Real Time Clock

S

- **Scheduling:** The general term used for programming something to happen on a preset schedule, such as Open/Close Schedules, Auto-Arming, Limited Access, and Relay Output Control.
- **Security Code:** a.k.a. user code; access code; Always 4 digits
- **Serial Programming:** * See Learn Mode
- **Siren:** A sounding device that consists of a speaker with a built-in siren driver
- **Siren Driver:** A device that sends electrical (Audio) signal to a speaker
- **Sniffer Mode:** Installer test modes used with wireless systems to determine if any other systems are operating in the immediate area, or to test reception of local transmitters.
- **Speaker (Loudspeaker):** A sounding device that consists of a paper cone and a magnetic coil through witch electrical signals are output as audible sounds
- **Split Reporting:** To send specific reports to one central station or receiver and other reports to a second central station or receiver
- **Standard Zones:** Zones that are available "out of the box"; zones that do not require the addition of expansion modules.
- **Stay Mode:** One of the arming modes; When armed stay, all perimeter zones are protected and all interior zones are bypassed
- **Strobe/Strobe light:** A high intensity light that flashes at a constant rate; rated in candle power or candela
- **Subscriber Account Number:** The 3-, 4-, or 10-digit number used by the central station to identify the particular account; this number is programmed into the control by the installer.
- **System Wide:** In partitioned systems this pertains to features and options that affect the system as a whole as opposed to only one partition (*see also partition specific)

T

- **Temporary Schedule:** Allows end user to override daily and holiday schedules for up to 1 week
- **Test Report Interval:** The programmable interval during which a periodic test report will be sent; Programmable in some controls for up to 1 month
- **Time Window:** A programmable period of time used with most scheduling features on some controls; Up to 20 time windows may be programmed for Open/Closing, Access Scheduling, etc.
- **Timers:** * See output timers and relays
- **Transmitter Test Mode:** This test mode allows the installer to verify that all programmed transmitters are being supervised by the system.
- **Two-way keypad:** A wireless keypad that both sends commands, and receives and displays the alarm status
- **Two-way Voice:** The ability for the central station to "listen-in" to the premise after an alarm

U

- **U.L.:** Underwriters Laboratory: Agency that lists products and system that have been tested and/or inspected to specific standards
- **Upload:** To get the program data over the phone line, IP connection, etc. from the control panel to the computer
- **User Code:** a.k.a. Access code, Security Code; Always 4-digits

V

- **Vista:** A line of Honeywell Panels

W

- **Wireless:** a.k.a. RF; Refers to the 5800/5700 series wireless transmitters and receivers
- **Wireless Button:** A 5800 Series Transmitter that employs buttons, such as a pendant or wireless key fob
- **Wireless Keys:** 5834-4 series wireless keys. A miniature programmable 4, button wireless key that can be connected to your keychain
- **Wireless Receiver:** Receivers for the 5800 wireless transmitters. They are classified as Low, Medium, or High. The low receiver can handle 8 wireless zones. The Medium receiver can handle 16 wireless zones. The high receiver can handle as many zones the panel has to offer. Receivers can be stand alone (5881, 5883) or built into a keypad (6150RF, 6160RF).

X

Y

Z

- **Zone List:** Used in conjunction with some scheduling features, on some controls, where the actions of specific zones can be used to control relay outputs and other events
- **Zone Response Type:** a.k.a. Zone Type: Each zone must be given a "personality"; each available zone type represents a different 'personality" such as a perimeter, interior, entry/exit, etc.

Section 11: Index

Section 12: Agency Statements

UL Installation Requirements

The following requirements apply to both UL Residential and UL Commercial Burglary installations:

- All partitions must be owned and managed by the same person(s).
- All partitions must be part of one building at one street address.
- The audible alarm device(s) must be placed where it/they can be heard by all partitions.
- The control cabinet must be protected from unauthorized access. This can be done by installing a tamper switch on the cabinet door (not supplied with VISTA-128BPT/VISTA-250BPT) or by installing a UL Listed passive infrared detector positioned to detect cabinet access. Wire the selected device to any EOLR-supervised zone (Zone 1-8). Program this zone for day trouble/night alarm (type 05) or 24-hour audible alarm (type 07) response. The 24-hour alarm response must be used for multiple-partitioned systems.
- Remote downloading and auto-disarming are not UL Listed features.

NOTE: UL Commercial Burglary installations require the attack resistant cabinet. The cabinet is included in the VISTA-ULKT kit.

UL609 Local Mercantile Premises/Local Mercantile Safe & Vault

Use the following guidelines for a Local Mercantile Premises/Local Mercantile Safe & Vault installation:

- All zones must be configured for EOLR supervision (*41=0). Wireless sensors may not be used. If 4190WH V-PLEXs are used set field *24 to "0" to enable tamper detection.
- Attach a door tamper switch (supplied) to the VISTA-128BPT/VISTA-250BPT cabinet backbox. For safe and vault installations, a shock sensor (not supplied) must also be attached to the backbox. (Also see *SECTION 3: Installing the Control*)
- Wire an ADEMCO AB12M Bell/Box to the bell output. Bell wires must be run in conduit. Program the bell output for a timeout of 16 minutes or longer timeout and for confirmation of arming ding. (Also see *SECTION 3: Installing the Control*.)
- Wire the VISTA-128BPT/VISTA-250BPT tamper switch and AB12M Bell/Box tamper switches to any EOLR-supervised zone (zones 1-8). Program this zone for day trouble/night alarm (type 05) or 24-hour audible alarm (type 07) response. The 24-hour alarm response must be used for multiple-partitioned systems.
- Entry delays must not exceed 45 seconds, and exit delays must not exceed 60 seconds.

UL365/UL609 Bank Safe and Vault Alarm System

- Follow the instructions for UL609 local installations above and Bank/Mercantile Safe and Vault (page 59) sections of this manual.
- Bell 1 Confirmation of Arming Ding (*16) must be set to 1 to on (enabled) (will automatically test bell).
- Entry delays or any other delays to report alarms may not exceed 45 seconds.
- Models 7847i, 7847i-E, IGSMV, and IGSMHS
- Bell Timeout must be programmed for 16 minutes min.
- Two 17.2AH Batteries must be used for this application.
- The main protective circuits, linings and attachments on the safe and vault, control units and alarm housing must be of the normally closed circuit, fully supervised type.
- To be installed inside the safe or vault.

UL365 Police Station Connected Burglar Alarm

Follow the instructions for UL609 local installations given above.

For Systems without Line Security:

- You may use the VISTA-128BPT/VISTA-250BPT dialer alone, or the 7847i Communicator alone.
- When using the dialer, program it to send Burglary Alarm, Low Battery, and Communicator Test reports. Field ∗27 must be set to "0024" (or less).
- If you are using the 7847i Communicator, connect it to the VISTA-128BPT/VISTA-250BPT burglary/audible panic alarm trigger.

For Systems with Line Security:

- You must use a GSMHS Communicator.

UL611/UL1610 Central Station Burglary Alarm

Follow the instructions for UL609 Local installations given above.

For Systems without Line Security:

- You must use the VISTA-128BPT/VISTA-250BPT' dialer with a 7847i Communicator.
- Connect the control's burglary/audible panic alarm trigger (on J7 header) and the 659EN's phone line monitor output to the 7847i. The 7847i will send a report to the central station when a telephone line fault condition is detected.
- Also connect the 7847i Communicator's fault output to one of the VISTA-128BPT/VISTA-250BPT EOLR-supervised zones (i.e., 1-8). Program this zone for a trouble by day/alarm by night (type 05) or a 24-hour alarm (type 07, 08) response to communicator's faults.
- Program the control's dialer to send Burglary Alarm, Trouble, Opening/Closing, and Low Battery reports.

For Systems with Line Security:

Follow the instructions for Systems without Line Security, except use the GSMHS Communicator in place of the 7847i.

California State Fire Marshal (CSFM) and UL Residential Fire Battery Backup Requirements

The California State Fire Marshal and UL have regulations that require all residential fire alarm control panels to have backup battery with sufficient capacity to operate the panel and its attached peripheral devices for 24 hours in the intended standby condition, followed by at least 4 minutes in the intended fire alarm signaling condition.

The VISTA-128BPT/VISTA-250BPT can meet this requirement without using a supplemental power supply, provided that the panel's outputs (including the current drawn from the auxiliary power output terminals) are limited as shown below:

- Output current is limited to 750mA maximum total auxiliary power, polling loop, and bell output current.
- Maximum auxiliary current is 300mA (including polling loop current).
- A 14AH battery is used. (Yuasa model NP7-12 recommended; use two connected in parallel.) A dual-battery harness is provided with ADEMCO No. 4100EOLR Resistor Kit (kit also contains EOL resistors having spade lug/heat shrink tubing construction approved by UL and CSFM for fire zone usage). Both batteries fit inside the panel's cabinet.

ULC Installation Requirements

- The zone inputs of the control unit are considered Low Risk applications only.
- The control unit must not be mounted on the exterior of a vault, safe or stockroom.
- Subscriber control units capable of maintaining opening (disarming) and closing (arming) schedules must facilitate a hardcopy printout of the opening (disarming) and closing (arming) schedule programming and of all the programmed holidays.
- Telephone service must be of the type that provides for timed release disconnect.
- A server employed for control over network addressing, encryption or re-transmission, Must be designed to remain in the "on state" at all times.
- Encryption must be enabled at all times for active communications channel security.
- For ULC Installations, refer to CAN/ULC-S302, Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults; CAN/ULC-S301, Standard for Central and Monitoring Station Burglar Alarm systems and CSA 22.1, Canadian Electrical Code, Part I, Safety Standard for Electrical Installations.

FEDERAL COMMUNICATIONS COMMISSION STATEMENTS

The user shall not make any changes or modifications to the equipment unless authorized by the Installation Instructions or User's Manual. Unauthorized changes or modifications could void the user's authority to operate the equipment.

FCC CLASS B STATEMENT

This equipment has been tested to FCC requirements and has been found acceptable for use. The FCC requires the following statement for your information:

This equipment generates and uses radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio and television reception. It has been type tested and found to comply with the limits for a Class B computing device in accordance with the specifications in Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- If using an indoor antenna, have a quality outdoor antenna installed.
- Reorient the receiving antenna until interference is reduced or eliminated.
- Move the radio or television receiver away from the receiver/control.
- Move the antenna leads away from any wire runs to the receiver/control.
- Plug the receiver/control into a different outlet so that it and the radio or television receiver are on different branch circuits.
- Consult the dealer or an experienced radio/TV technician for help.

INDUSTRY CANADA CLASS B STATEMENT

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

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

FCC/IC STATEMENT

This device complies with Part 15 of the FCC Rules, and Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference (2) This device must accept any interference received, including interference that may cause undesired operation.

Cet appareil est conforme à la partie 15 des règles de la FCC & de RSS 210 des Industries Canada. Son fonctionnement est soumis aux conditions suivantes: (1) Cet appareil ne doit pas causer d' interferences nuisibles. (2) Cet appareil doit accepter toute interference reçue y compris les interferences causant une reception indésirable.

IN THE EVENT OF TELEPHONE OPERATIONAL PROBLEMS

In the event of telephone operational problems, disconnect the control panel by removing the plug from the RJ31X (CA38A in Canada) wall jack. We recommend that you demonstrate disconnecting the phones on installation of the system. Do not disconnect the phone connection inside the control panel. Doing so will result in the loss of your phone lines. If the regular phone works correctly after the control panel has been disconnected from the phone lines, the control panel has a problem and should be returned for repair. If upon disconnection of the control panel, there is still a problem on the line, notify the telephone company that it has a problem and request prompt repair service. The user may not under any circumstances (in or out of warranty) attempt any service or repairs to the system. It must be returned to the factory or an authorized service agency for all repairs.

FCC PART 68 NOTICE

This equipment complies with Part 68 of the FCC rules. On the front cover of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

This equipment uses the following jacks:

An RJ31X is used to connect this equipment to the telephone network.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact the manufacturer for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request that you remove the equipment from the network until the problem is resolved.

There are no user serviceable components in this product, and all necessary repairs must be made by the manufacturer. Other repair methods may invalidate the FCC registration on this product.

This equipment cannot be used on telephone company-provided coin service. Connection to Party Line Service is subject to state tariffs.

This equipment is hearing-aid compatible.

When programming or making test calls to an emergency number, briefly explain to the dispatcher the reason for the call. Perform such activities in the off-peak hours, such as early morning or late evening.

CANADIAN EMISSIONS STATEMENTS

Ringer Equivalence Number Notice:

The **Ringer Equivalence Number** (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

AVIS : L'indice d'équivalence de la sonnerie (IES) assigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent être raccordés à une interface. La terminaison d'une interface téléphonique peut consister en une combinaison de quelques dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

Section 13: System Commands

User Code Commands	Add A User Code = User Code + 8 + New User Number + New User's Code Change a Code = User Code + 8 + User Number + New User's Code Delete a User's Code = Your User Code + 8 + User Number to Be Deleted + Your Code Again View User Capability = User's Code + [*] + [*] Set Real-Time Clock (Installer, Master Only) = Code + [#] + 63	
Programming Commands	Site Initiated Download = User Code + [#] + 1. Activate Panel initiated Communication Session with Compass via the Dialer = Installer Code + [#] + 1. Direct-Wire Download Enable = User Code + [#] + 5. Enter Program Mode = Installer Code + 8000. Enter Interactive Program Mode = Installer Code + 8000 + [#] + 93 Exit Program Mode = *99 or *98.	
Event Logging Commands	Event Log Display = Code + [#] + 60 (Installer or Master Only) Event Log Print = Code + [#] + 61 (Installer or Master Only) Clear Event Log = Code + [#] + 62 (Installer or Master Only)	
Wireless System Commands	House ID Sniffer Mode = Code + [#] + 2 (Installer Only) Transmitter ID Test = Code + [#] + 3 (Installer Only) Go/No Go Test = Code + 5 (Test Key)	
Additional Commands	Partition GOTO	User Code + [*] + Partition Number 0-8.
	GOTO Home Partition	User Code + [*] + 0.
	Panics	[*] + 1 or A Key (Zone 995). [*] + [#] or B Key (Zone 999). [#] + 3 or C Key (Zone 996).
	View Downloaded Messages	Press 0 for 5 Seconds.
	Display All Zone Descriptors	Press [*] for 5 Seconds.
Output Device Control Commands	Activate Output Device as Programmed = User Code + [#] + 71. Activate Output Device as Programmed = User Code + [#] + 72. Activate Output Device Manually = User Code + [#] + 70. Activate Output Device or System Event Instantly = User Code + [#] + 77. Randomize Output Devices = User Code + [#] + 41 Randomize Output Devices Programmed with Activation Times Between 6 PM and 5 AM = User Code + [#] + 42. De-activate Randomization = Enter the sequence used to activate randomization.	
Scheduling Commands	Installer-Programmed Schedule Events = Installer Code + [#] + 80 (Installer or Master Only). Temporary Schedule Editing = User Code + [#] + 81 (Installer, Master, Manager Only). Extend Closing Window = User Code + [#] + 82 (Installer, Master, Manager Only). End User Output Device Programming = User Code + [#] + 83.	
Access Control Commands	Activate Access Relay for Current Partition = User Code + 0. Request to Enter/Exit = User Code + [#] + 73. Request to Enter/Exit at Access Point = User Code + [#] + 74 + Access Point Number. Change Access Point State = User Code + [#] + 75 + Access Point + State. Perform a Test of the VistaKey Module = Installer Code + [#] + 78. Perform an Access Control Card Function = User Code + [#] + 79.	
Master Code + # + 65	If local programming lockout is set via downloading, programming mode cannot be entered at the keypad unless Master Code + #65 is entered, which opens up a 24hr window to allow the installer to enter the program mode. Once the 24hrs has expired the program mode is again locked out.	

Section 14: Specifications

VISTA-128BPT/VISTA-250BPT CONTROL

Physical:

Standard Cabinet (included)	12 1/2" W x 14 1/2" H x 3" D
UL Cabinet (optional)	14 1/2" W x 18" H x 4.3" D (Included in the COM-UL Commercial Enclosure)

Electrical:

Voltage Input: in	From ADEMCO No. 1361/1361-GT Plug-In Transformer (use 1361CN/1361CN-GT Canada) rated 16.5VAC, 40 VA.
Alarm Sounder Output:	10VDC-13.8VDC, 1.7A max. (UL1023, UL609 installations); 750mA less aux. current draw (UL985 installations).
Auxiliary Power Output:	9.6VDC-13.8VDC, 750mA max. For UL installations, the accessories connected to the output must be UL Listed, and rated to operate in the above voltage range.
Backup Battery:	12VDC, 4AH or 7AH gel cell. YUASA NP4-12 (12V, 4AH) or NP7-12 (12V, 7AH) recommended.
Standby Time:	4 hours min. with 750 mA aux. load using 7 AH battery.
Circuit Protectors:	PTC circuit breakers are used on battery input to protect against reverse battery connections and on alarm sounder output to protect against wiring faults (shorts). A solid-state circuit breaker is used on auxiliary power output to protect against wiring faults (shorts).

Digital Communicator

Formats Supported:	4 + 2 Express, Contact ID and 10-Digit Contact ID
Line Seize:	Double Pole
Ringer Equivalence:	0.7B
FCC Registration No.:	AC398U-68192-AL-E

Remote Keypads

6160

Physical:

Width:	7.437 in.
Height:	5.25 in.
Depth:	1.312 in.

Electrical:

Voltage Input:	12VDC
Current Drain:	150mA

Interface Wiring:

RED:	12VDC input (+) auxiliary power
GREEN:	Data to control panel
YELLOW:	Data from control panel
BLACK:	Ground and (-) connection from supplemental power supply

6160V

Physical:

Width:	7 3/8 inches
Height:	5 5/16 inches
Depth:	1 3/16 inches

Electrical:

Voltage Input:	12VDC
Current Drain:	190mA

Interface Wiring:

RED:	12VDC input (+) auxiliary power
GREEN:	Data to control panel
YELLOW:	Data from control panel
BLACK:	Ground and (-) connection from supplemental power supply

Section 15: Contact ID Codes

Table of Contact ID Codes

Code	Definition
110	Fire Alarm
111	Smoke Alarm
121	Duress
122	Silent Panic
123	Audible Panic
124	Duress Access Grant
125	Duress Egress Grant
131	Perimeter Burglary
132	Interior Burglary
133	24-Hour Burglary
134	Entry/Exit Burglary
135	Day/Night Burglary
140	ACS Zone Alarm
150	24-Hour Auxiliary
162	CO Alarm
301	AC Loss
302	Low System Battery
305	System Reset
306	Program Tamper
308	System Shutdown
309	Battery Test Fail
313	System Engineer Reset
320	ACS Relay Supervision
321	Bell 1 Trouble
332	Poll Loop Short-Trouble
333	Expansion Module Failure
338	ACS Module Low Battery
339	ACS Module Reset
342	ACS Module AC Loss
343	ACS Module Self-Test Fail
344	RF Receiver Jam Detect
354	Dialer Queue Overflow
373	Fire Loop Trouble
374	Exit Error by Zone
378	Cross Zone Trouble
380	Trouble (global)
381	Loss of Supervision (RF)
382	Loss of RPM Supervision
383	RPM Sensor Tamper
384	RF Transmitter Low Battery
385	Smoke Detector HI
386	Smoke Detector LO
389	Detector Self-Test Failed
401	O/C by User
403	Power-Up Armed/Auto-Arm
406	Cancel by User
407	Remote Arm/Disarm (Download)
408	Quick Arm
409	Keyswitch O/C
411	Callback Requested
421	Access Denied
422	Access Granted
423	Door Force Open
424	Egress Denied
425	Egress Granted
426	Door Prop Open
427	Access Point DSM Trouble
428	Access Point RTE Trouble
429	ACS Program Entry
430	ACS Program Exit
431	ACS Threat Change
432	Access Point Relay/Trigger Fail
433	Access Point RTE Shunt
434	Access Point DSM Shunt/Unshunt
441	Armed STAY
451	Early Open/Close
452	Late Open/Close
453	Fail to Open
454	Fail to Close
455	Auto-Arm Fail
459	Recent Close
501	ACS Reader Disable
520	ACS Relay Disable
570	Bypass
576	ACS Zone Shunt
577	ACS Point Bypass
579	Vent Zone Bypass
601	Panel Test via Compass Software
602	Communicator Test
606	Listen-In to Follow
607	Burglary Walk-Test
621	Event Log Reset
625	Time/Date Reset
631	Exception Schedule Change
632	Access Schedule Change

NOTE: If 2*03 ULC S304 feature is enabled and there is a phone line (or radio) failure and the panel has exhausted its maximum attempts to send reporting events to the central station, the panel will hold the messages in a buffer and resend upon restoral of the communication path. In addition, old messages that are sent will indicate that they are not current messages so that the central station does not dispatch on them.

In order to accomplish this, an event qualifier of "6" will be sent in place of the "1" or "3" character in the message. The "6" indicates that the message is old. Events will be sent in chronological order and will be time-stamped in the system's event log.

Section 16: Event Log Descriptions

Event Log Alpha Descriptors

Alpha	Event Description
FIRE	Fire Alarm
DURESS	Duress Alarm
PANIC	Silent or Audible Panic Alarm
BURGLARY	Burglary Alarm
EXP SHRT	Polling Loop Short
RF EXPND	Expander Module Failure
AUXILIARY	Non-burglary Alarm
TROUBLE	Trouble
AC LOSS	AC Loss
LOW BATTERY	System Low Battery
SYSTEM RESET	System Reset
PROG CHANGE	Program Change
BATTERY FAIL	System Battery Failure
RF SUPR	RF Supervision
RPM SUPR	RPM Supervision
RF LBAT	RF Low Battery
EXP TRBL	Expander Module Trouble
RF TRBL	RF Trouble
TAMPER	Tamper
FIRE TRB	Fire Trouble
FAIL TO COMM	Failure to Communicate
BELL TROUBLE	Bell Trouble
DISARMED	Disarmed
DISARMED-REM	Disarmed Remotely
DISARMED-KEY	Disarmed Via RF Key
DISARM-AUTO	Auto-Disarm
CALL BACK	Callback Requested
CANCEL	Cancel
DISRMD-EARLY	Disarmed Early
DISRMD-LATE	Disarmed Late
MISSED DISRM	Missed Disarm
SKED CHANGE	Schedule Change
ACC SKED CHG	Access Control Schedule Change
ARM FAILED	Failed to Arm
DIALER SHUT	Dialer Shutdown
SYSTEM SHUT	System Shutdown
BYPASS	Bypass
SELF TEST	Self-test
TEST ENTRY	Manual Test Entry
TEST EXIT	Manual Test Exit
LOG OVERFLOW	Dialer Queue Overflow

Alpha	Event Description
LOG CLEARED	Event Log Cleared
TIME SET	Time Set
TIME ERROR	Time Error
PROGRM ENTRY	Program Entry
PROGRAM EXIT	Program Exit
Uxxx ADD BY	User XXX Added BY
Uxxx DEL BY	User XXX Deleted BY
Uxxx CHG BY	User XXX Changed BY
PRINTER FAIL	Event Log Printer Failure
TESTED	Zone Tested
UNTESTED	Zone Untested
FAILED	Zone Test Failed
RLY TRBL	Relay Trouble
EXP TMPR	Expansion Module Tamper
VENT BYPASS	Vent Zone Bypass
RF JAM	RF Jam Detected
JAM RSTR	RF Jam Restore
FIRE RST	Fire Alarm Restore
DURE RST	Duress Alarm Restore
PNC RST	Panic Alarm Restore
BURG RST	Burglary Alarm Restore
EXP RST	Expansion Module Restore
RF RST	RF Restore
AUX RST	Auxiliary Restore
MED RST	Medical Restore
TRBL RST	Trouble Restore
AC RESTORE	AC Restore
LOW BATT RST	System Low Battery Restore
PROG CHANGE	Program Change
BAT TST FAIL	Battery Test Failure
RPM RST	V-PLEX Restore
RFLB RST	RF Low Battery Restore
EXP RST	Expansion Module Failure Restore
TMPR RST	Tamper Restore
FRTR RST	Fire Trouble Restore
COMM RESTORE	Communication Restore
RLY RST	ECP Relay Trouble Restore
ARMED	Armed
ARMED-STAY	Armed Stay
ARMED-REM	Armed Remotely
ARMED-QUICK	Quick Armed

Alpha	Event Description
ARMED-KEY	Armed Via RF Key
ARMED-AUTO	Auto-Armed
PARTIAL ARM	Partial Armed
ARMED-EARLY	Armed Early
ARMED-LATE	Armed Late
MISSED ARM	Missed Arm
DIALER RST	Dialer Restore (Shutdown)
SYSTEM RST	System Restore (Shutdown)

Alpha	Event Description
BYP RST	Bypass Restore
TEST EXIT	Test Mode Exit
PRINTER RSTR	Printer Restore
BELL RESTORE	Bell Restore
EXIT ERR	Exit Error
RECENT ARM	Recent Arm
VENT BYP RST	Vent Zone Bypass Restore
DIALER FULL	Dialer Overflow

Access Control Events

Alpha	Event Description
ACS PNT	Access Point Failure
DSM SHNT	Door Status Monitor Shunt
DUR ACCS	Duress Access Grant
NO ENTRY	Access Denied
DR OPEN	Door Propped Open
DR FORCE	Door Forced Open
ENTERED	Access Granted
NO EXIT	Egress Denied
ACPT BYP	Access Point Bypass
RTE SHNT	Request to Exit Shunt
EXITED	Egress Granted
ACLO MOD	AC Loss at Module
LBAT MOD	Low Battery at Module
COMM MOD	Comm Failure from MLB to Module
RES MOD	Access Control Module Reset
ACPT RLY	Access Point Relay Supervision Fail
SELF MOD	Module Self-Test Failure
ACZN CHG	Access Control Zone Change
ACS PROG	Access Control Program Entry
ACS PRGX	Access Control Program Exit
THRT CHG	Access Control Threat Change
SYS SHUT	System Shutdown
SYS RST	System Engineer Reset
ZN SHUNT	Access Control Zone Shunt
ZN ALARM	Access Control Zone Alarm
RDR DISA	Access Control Reader Disable

Alpha	Event Description
RLY DISA	Access Control Relay/Trigger Disable
RTE TRBL	Request to Exit Point Trouble
DSM TRBL	Door Status Monitor Point Trouble
DUR EXIT	Duress Egress Grant
BGN ACS TEST	Access Control Test Mode Start
ACPT RST	Access Point Restore
ACRST MOD	AC Loss at Module Restore
LBAT RST	Low Battery at Module Restore
COMM RST	Comm Fail MLB to Module Restore
RLY RST	Access Point Relay Supervision Rest
SELF RST	Self-Test at Module Restore
ACPT UNB	Access Point Unbypass
DSM UNSH	Door Status Monitor Unshunt
RTE UNSH	Request to Exit Point Unshunt
DRFO RST	Door Forced Open Restore
DRPO RST	Door Propped Open Restore
DSM RST	Door Status Monitor Trouble Restore
RTE RST	Request to Exit Point Trouble Rest
RLY ENAB	Access Control Relay/Trigger Enable
RDR ENAB	Access Control Reader Enable
ZNAL RST	Access Control Zone Restore
ZN UNSHT	Access Control Zone Unshunt
SYSHTRST	System Shutdown Restore
END ACS TEST	Access Control Test Mode End

VISTA-128BPT Summary of Connections

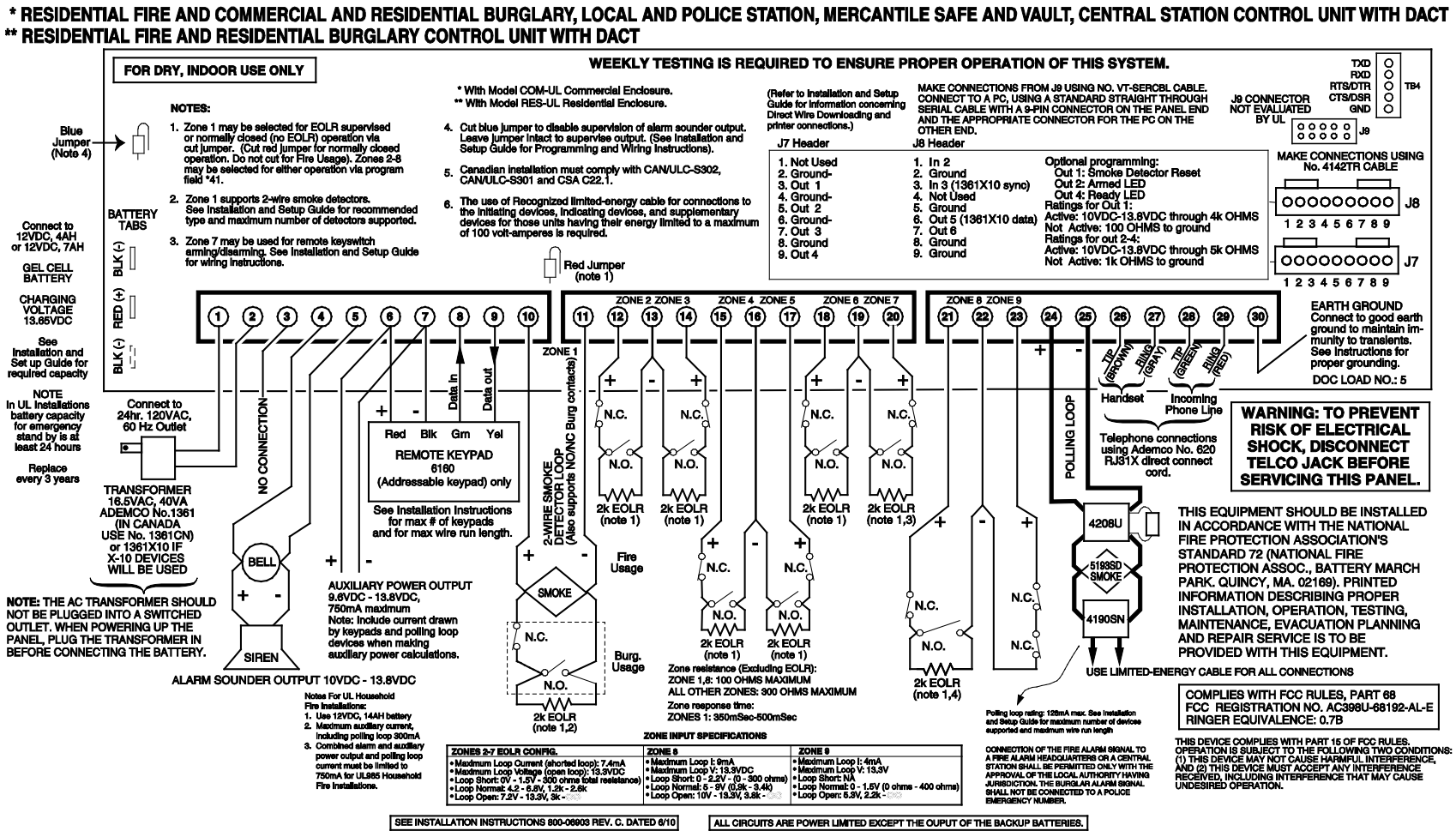


Figure 39: VISTA-128BPT SOC

VISTA-250BPT Summary of Connections

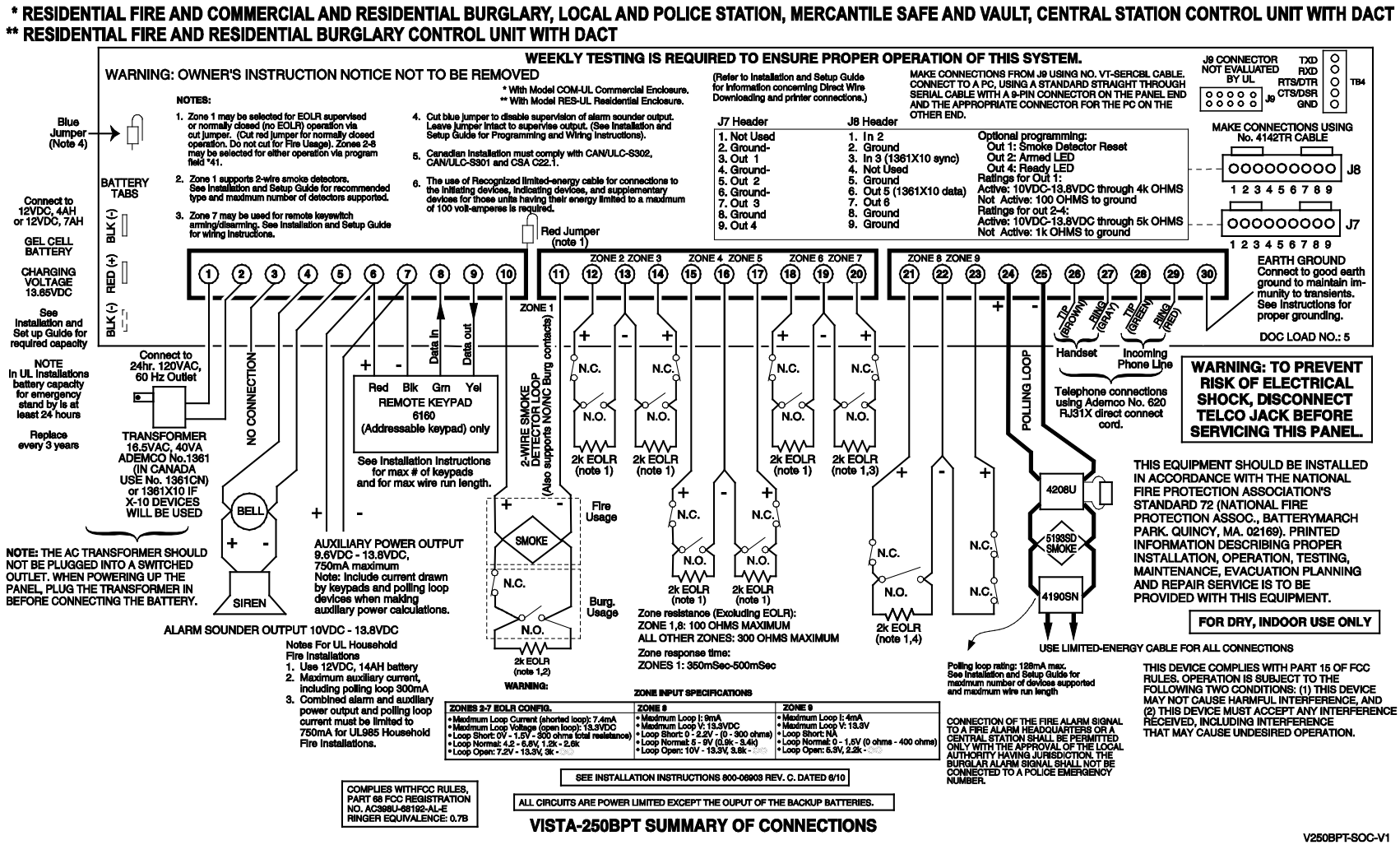
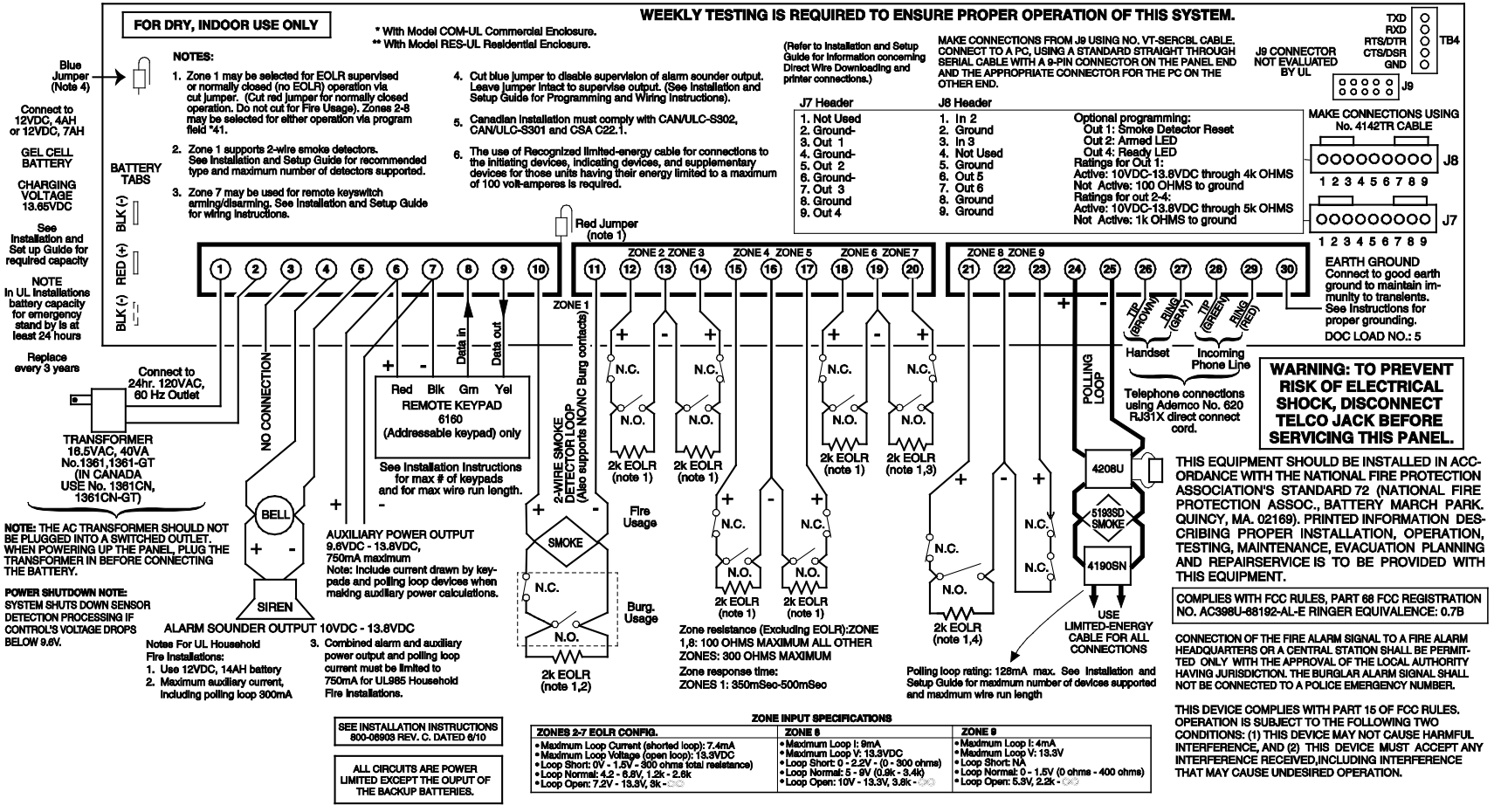


Figure 40: VISTA-250BPT SOC

VISTA-128BPTSIA Summary Of Connections

*** RESIDENTIAL FIRE AND COMMERCIAL AND RESIDENTIAL BURGLARY, LOCAL AND POLICE STATION, MERCANTILE SAFE AND VAULT, CENTRAL STATION CONTROL UNIT WITH DACT**
**** RESIDENTIAL FIRE AND RESIDENTIAL BURGLARY CONTROL UNIT WITH DACT**



VISTA-128BPTSIA SUMMARY OF CONNECTIONS

V128BPTSIA-SOC-V2

Figure 41: VISTA128BPTSIA SOC

NOTES

NOTES

NOTES

NOTES

NOTES

WARNING!
THE LIMITATIONS OF THIS ALARM SYSTEM

While this System is an advanced wireless security system, it does not offer guaranteed protection against burglary, fire or other emergency. Any alarm system, whether commercial or residential, is subject to compromise or failure to warn for a variety of reasons. For example:

- Intruders may gain access through unprotected openings or have the technical sophistication to bypass an alarm sensor or disconnect an alarm warning device.
- Intrusion detectors (e.g., passive infrared detectors), smoke detectors, and many other sensing devices will not work without power. Battery-operated devices will not work without batteries, with dead batteries, or if the batteries are not put in properly. Devices powered solely by AC will not work if their AC power supply is cut off for any reason, however briefly.
- Signals sent by wireless transmitters may be blocked or reflected by metal before they reach the alarm receiver. Even if the signal path has been recently checked during a weekly test, blockage can occur if a metal object is moved into the path.
- A user may not be able to reach a panic or emergency button quickly enough.
- While smoke detectors have played a key role in reducing residential fire deaths in the United States, they may not activate or provide early warning for a variety of reasons in as many as 35% of all fires, according to data published by the Federal Emergency Management Agency. Some of the reasons smoke detectors used in conjunction with this System may not work are as follows. Smoke detectors may have been improperly installed and positioned. Smoke detectors may not sense fires that start where smoke cannot reach the detectors, such as in chimneys, in walls, or roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level of a residence or building. A second floor detector, for example, may not sense a first floor or basement fire. Finally, smoke detectors have sensing limitations. No smoke detector can sense every kind of fire every time. In general, detectors may not always warn about fires caused by carelessness and safety hazards like smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches, or arson. Depending on the nature of the fire and/or location of the smoke detectors, the detector, even if it operates as anticipated, may not provide sufficient warning to allow all occupants to escape in time to prevent injury or death.
- Passive Infrared Motion Detectors can only detect intrusion within the designed ranges as diagrammed in their installation manual. Passive Infrared Detectors do not provide volumetric area protection. They do create multiple beams of protection, and intrusion can only be detected in unobstructed areas covered by those beams. They cannot detect motion or intrusion that takes place behind walls, ceilings, floors, closed doors, glass partitions, glass doors, or windows. Mechanical tampering, masking, painting or spraying of any material on the mirrors, windows or any part of the optical system can reduce their detection ability. Passive Infrared Detectors sense changes in temperature; however, as the ambient temperature of the protected area approaches the temperature range of 90° to 105°F (32° to 40°C), the detection performance can decrease.
- Alarm warning devices such as sirens, bells or horns may not alert people or wake up sleepers if they are located on the other side of closed or partly open doors. If warning devices are located on a different level of the residence from the bedrooms, then they are less likely to waken or alert people inside the bedrooms. Even persons who are awake may not hear the warning if the alarm is muffled by noise from a stereo, radio, air conditioner or other appliance, or by passing traffic. Finally, alarm-warning devices, however loud, may not warn hearing-impaired people.
- Telephone lines needed to transmit alarm signals from a premises to a central monitoring station may be out of service or temporarily out of service. Telephone lines are also subject to compromise by sophisticated intruders.
- Even if the system responds to the emergency as intended, however, occupants may have insufficient time to protect themselves from the emergency situation. In the case of a monitored alarm system, authorities may not respond appropriately.
- This equipment, like other electrical devices, is subject to component failure. Even though this equipment is designed to last as long as 20 years, the electronic components could fail at any time.

The most common cause of an alarm system not functioning when an intrusion or fire occurs is inadequate maintenance. This alarm system should be tested weekly to make sure all sensors and transmitters are working properly. The security keypad (and remote keypad) should be tested as well.

Wireless transmitters (used in some systems) are designed to provide long battery life under normal operating conditions. Longevity of batteries may be as much as 4 to 7 years, depending on the environment, usage, and the specific wireless device being used. External factors such as humidity, high or low temperatures, as well as large swings in temperature, may all reduce the actual battery life in a given installation. This wireless system, however, can identify a true low battery situation, thus allowing time to arrange a change of battery to maintain protection for that given point within the system.

Installing an alarm system may make the owner eligible for a lower insurance rate, but an alarm system is not a substitute for insurance. Homeowners, property owners and renters should continue to act prudently in protecting themselves and continue to insure their lives and property. We continue to develop new and improved protection devices. Users of alarm systems owe it to themselves and their loved ones to learn about these developments.

Honeywell

2 Corporate Center Drive, Suite 100
P.O. Box 9040, Melville, NY 11747

www.honeywell.com/security

SUPPORT, WARRANTY, & PATENT INFORMATION

For the latest documentation and online support information, please go to:
https://mywebtech.honeywell.com/

For the latest warranty information, please go to:
www.honeywell.com/security/hsc/resources/wa.

For patent information, see
www.honeywell.com/patents

MyWebTech

Warranty

Patents

800-06903V4 10/16 Rev B