

JCI Security Products

Publications Cover Sheet

JCI Pubs Owner: Ian Woolard

Part Number: 29010933R003

Revision: 003

Release Number: 14335

Notes: Publication for Online Only - Added list of warnings applicable when this equipment is connected to the New Zealand Telecom Network.

Description: POWERSERIES PRO HS3032/HS3128/HS3248 V1.3 ONLINE USER MANUAL ENG [HS3XXX v1.3 UM ENG]

Type: Electronic Media

Pieces:

Printing Instructions: Not Required



PowerSeries Pro HS3032/HS3128/HS3248 User Manual



HS3032, HS3128, HS3248



29010933R003



Contents

Quick reference.....	7
Safety instructions.....	9
The PowerSeries Pro security system.....	10
General system operation.....	10
Carbon monoxide detection.....	10
Fire detection.....	10
Testing the system.....	10
Performing a keypad and siren test.....	11
Monitoring.....	11
Maintenance.....	11
Applicable models.....	11
Securing the premises.....	13
Arming the system.....	13
Arming the system in Away mode using a keypad.....	13
Arming the system in Away mode.....	13
Canceling the arming sequence.....	14
Arming the system in Stay mode.....	14
Canceling the arming sequence.....	15
Silent exit delay.....	15
Arming the system with a wireless key.....	15
Arming the system with a proximity tag.....	15
Night arming.....	15
Arming the system in Night mode.....	16
Disarming a system that is in Night mode.....	16
No-entry arming.....	16
Arming the system using the No-entry arm feature.....	16
Canceling the arm sequence.....	16
Exit Delay Time Restart.....	16
The Quick Exit feature.....	17
Exiting the premises using the Quick Exit feature.....	17
Bypassing zones.....	17
Additional bypass features.....	18
Bypassing individual zones.....	18
Bypassing all open zones.....	18
Recalling the last bypassed zones.....	19
Clearing the bypass indication from all zones.....	19
Bypass groups.....	19
Programming a bypass group.....	19
Loading a bypass group.....	20
Arming troubles and exit faults.....	20
Arming troubles.....	20

Correcting an arming error.....	20
Audible exit faults.....	20
Correcting an exit fault.....	21
Disarming the system.....	21
Disarming the system with a keypad.....	21
Disarming the system with a wireless key.....	21
Disarming the system with a proximity tag.....	21
Disarming error.....	21
Alarms.....	22
Using emergency keys.....	22
Fire alarm.....	22
Silencing a fire alarm.....	22
Bells Silenced LCD display for fire alarms.....	22
Resetting smoke detectors.....	23
Carbon monoxide alarm.....	23
Bells Silenced LCD display for CO alarms.....	23
Intrusion and burglary alarm.....	23
Alarm Cancel window.....	24
Viewing alarms in memory.....	24
Alarm messages.....	24
Wireless keys.....	25
Using wireless keys.....	25
Using Proximity Tags.....	25
Managing Users.....	26
Access code types.....	26
Opening the access codes menu.....	27
Adding, changing, and deleting access codes.....	27
Adding or changing a user access code.....	27
Enrolling a proximity tag.....	28
Deleting a proximity tag.....	28
User labels.....	29
Adding and editing a user label.....	29
Assigning a partition to a user code.....	29
Configuring additional user options.....	30
Accessing the user function menu.....	31
Viewing the event buffer.....	32
Setting the time and date.....	32
Configuring the auto arm and disarm feature.....	32
Setting the auto arm time.....	32
Disabling the auto arm time.....	33
Configuring the system service DLS.....	33
User Callup.....	33

Configuring the late to open feature.....	33
Setting the late to open time feature.....	34
Disabling the late to open time feature.....	34
Changing the brightness of the LCD keypad.....	34
Changing the contrast of the LCD keypad.....	34
Setting the buzzer volume.....	35
Setting the voice prompt volume.....	35
Setting the voice chime volume.....	35
Resetting the system.....	35
Engineer's reset.....	35
Remote (anti-code) reset.....	35
Initiating a walk test.....	36
Canceling a walk test.....	37
Managing partitions.....	38
Partitions.....	38
Single partition operation.....	38
Loaning a keypad to another partition.....	38
Fire and CO zone types.....	39
Additional features.....	40
Viewing a temperature in a zone.....	40
Turning the chime on or off.....	40
Audio verification.....	40
Visual verification.....	40
Video on demand.....	40
PIR camera zone association.....	40
Activating a command output.....	41
Configuring a command output to follow a schedule.....	41
Burglary verification.....	41
Call waiting.....	41
Fire alarm verification.....	41
System lockout due to invalid attempts.....	41
Troubleshooting.....	43
Trouble conditions.....	43
Reference sheets.....	47
System information.....	47
Service contact information.....	47
Access codes.....	48
Sensor and zone information.....	49
Locating detectors and escape plan.....	50
Smoke detectors.....	50
Fire escape planning.....	52

Carbon monoxide detectors..... 53

Quick reference

The PowerSeries Pro alarm system uses shortcut keys to access options or features on all models of keypads. When using an LCD keypad, the PowerSeries Pro alarm system additionally uses a menu based navigation system. Use the scroll keys to view the list of options contained within the current menu.

- ① **Note:** Some features must be enabled by the installer.
- ① **Note:** Bypass Groups are not permitted in UL listed installations.

For SIA CP-01 classified installations, the Swinger Shutdown feature shall shut down the zone after a programmable number of trips (the programmed default is 2). The zone is restored after a manual reset by entering the access code at the time of disarming the alarm system, or it is reset automatically after 48 hours with no trips on any zones.

The following tables provides an overview of the keypad status lights and keys.

Table 1: Keypad status lights



































Status light	Name	Description
	Ready	Indicates that the system is ready to arm. To arm the system this light must be on, and all zones must be secure or bypassed.
	Armed	Indicates that the system is armed. If the Ready light and the Armed light are both turned on, an Exit Delay is in progress.
	Trouble	Indicates that there is a system malfunction or a tamper issue. If the Trouble light flashes, the keypad has a low battery condition. Correct the trouble condition to turn off this light. For more information on correcting trouble conditions, see Troubleshooting .
	AC power	Indicates that AC power is connected. The AC power light turns off when the AC power is disconnected.

Table 2: Keypad keys

Key	Key name	Key type
	Stay arm	Function
	Away arm	Function
	Chime	Function
	Reset	Function
	Quick exit	Function
	Fire alarm	Emergency
	Medical alarm	Emergency
	Panic alarm	Emergency

Action	Press
Arming and Disarming	
Away arm	 for 2 seconds + [Access Code†]
Stay arm	 for 2 seconds + [Access Code†]
Night Arm	When Armed in stay mode [*][1] + [Access Code†]
Disarm	[Access Code]
No-Entry Arming	[*][9] + [Access Code†]
Quick arm	When the system is disarmed, press * 0
Quick exit	When the system is armed, press * 0
Cancel arm Sequence	[Access Code]
Bypassing - All bypass commands begin with [*][1] + [Access Code†]	
Bypass Individual Zones	[3 Digit Zone #]
Bypass All Open Zones	[9][9][8]
Recall Last Bypass	[9][9][9]
Clear Bypass	[0][0][0] OR [Scroll] Bypass Options + [*] +   Clear Bypasses + [*]
Program Bypass Group	[3 digit zone #s] + [9][9][5] OR [3 digit zone #s] +   Bypass Options + [*] +   Prg Bypass Group + [*]
Load Bypass Group	[9][9][1] or   Bypass Options + [*] + [Scroll] Bypass Group + [*]
Common Functions	
Set Time and Date	[*][6] [Master Code] + [0][1]
Turn Chime ON/OFF	[*][4] + [Access Code†] or 
Change Brightness	[*][6] [Master Code] + [1][2] +  
Change Contrast	[*][6] [Master Code] + [1][3] +  
Buzzer Volume	[*][6] + [Master Code] + [1][4] +  
Add/Delete User	[*][5] + [Master Code] + [Access Code] + 1
Reset Smoke Detectors	 OR [*][7][2]
View Troubles	[*][2] + [Access Code†] +  
View Alarms	[*][3] + [Access Code†] +  
Performing a system test	[*][6] + [Master Code] + [0][4]

† If configured by the installer.

Safety instructions

- ▶ **Important:** This equipment must be installed by a skilled person only. A skilled person is an installer with appropriate technical training. The installer must be aware of potential hazards during installation and measures available to minimize risks to the installer and other people.

There are no user serviceable parts in this equipment. All equipment must be serviced by a skilled person.

The PowerSeries Pro security system

The PowerSeries Pro has been designed to provide the greatest possible flexibility and convenience. Read this manual carefully and have the installer provide instructions on how to operate the system and which features have been implemented. All users of this system should be equally instructed in its use.

Fill out the **System Information** section with zone information and access codes and store this manual in a safe place for future reference.

- ① **Note:** The PowerSeries Pro security system includes specific false alarm reduction features and is classified in accordance with ANSI/ SIA CP-01-2014 Control Panel Standard - Features for False Alarm Reduction. Please consult the installer for further information regarding false alarm reduction features built into the system as all are not covered in this manual.

General system operation

This security system is made up of a PowerSeries Pro control panel, one or more keypads and various sensors and detectors. The metal enclosure contains the system electronics and standby battery. The keypad is used to send commands to the system and to display the current system status. The keypad(s) are mounted in a convenient location inside the protected premises close to the entry/exit door(s). The security system has several zones of area protection, each connected to one or more sensors (motion detectors, glassbreak detectors, door contacts, etc.).

- ① **Note:** Only the installer or service professional shall have access to the control panel.

Carbon monoxide detection

This equipment is capable of monitoring carbon monoxide detectors and providing a warning if carbon monoxide is detected. Please read the Escape Planning guidelines in this manual and instructions that are available with the carbon monoxide detector.

- ① **Note:** Must be enabled and configured by installer.
- ① **Note:** The equipment should be installed in accordance with NFPA 720.

Fire detection

This equipment is capable of monitoring fire detection devices such as smoke detectors and providing a warning if a fire condition is detected. Good fire detection depends on having adequate number of detectors placed in appropriate locations. This equipment should be installed in accordance with NFPA 72 (N.F.P.A., Batterymarch Park, Quincy MA 02269). Carefully review the Escape Planning guidelines in this manual.

- ① **Note:** Must be enabled and configured by installer.

Testing the system

Perform a system test to test all system keypad LEDs, keypad sounders, bells and sirens. To ensure the system continues to function as intended, test your system weekly.

- **Important:** For UL HOME HEALTH CARE listed applications the system shall also be tested weekly without AC power. To remove AC from the control unit, remove the screw from the restraining tab of the plug in adapter and remove the adapter from AC outlet. After completing the test of the unit using only the battery backup source, reconnect the plug in adapter and attach the screw through the restraining tab so that the adapter is securely attached to the outlet.

If the system fail to function properly contact the installation company.

- **Important:** You must test all the smoke detectors yearly.

Performing a keypad and siren test

To perform a keypad and siren test, complete the following steps:

1. On the keypad, press * 6.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **System Test**, and press *. All keypad sounders, bells, sirens, and keypad LEDs activate for 2 seconds.
4. Press # to return to the ready state.

Monitoring

This system is capable of transmitting alarms, troubles and emergency information. If an alarm is initiated by mistake, immediately call the central station to prevent an unnecessary response.

- ① **Note:** For CP-01 systems, the monitoring function must be enabled by the installer before it is operational. There is a communicator delay of 30 seconds in this control panel. It can be removed, or it can be increased up to 45 seconds, at the option of the end-user by consulting with the installer. Fire type alarms are normally reported without a delay.

Maintenance

Keep your alarm controller in optimal condition by following the instructions included within this manual and/or marked on the product. The end user and/or installer are responsible for disposing of used batteries according to local waste recovery and recycling regulations.

- Use the system test described in “Testing the System” to check the battery condition. For optimal performance, replace the standby batteries every 3-5 years.
- For other system devices such as smoke detectors, motion detectors or glassbreak detectors, consult the manufacturer’s literature for testing and maintenance instructions.
- Lightly dust the security equipment with a slightly moistened cloth.
- ① **Note:** Do not use abrasives, thinners, solvents or aerosol cleaners (spray polish) that may enter through holes in the Alarm Controller and cause damage. Do not wipe the front cover with alcohol, water or any other liquid.

Applicable models

This publication covers the following models:

- ① **Note:** The X character refers to one of the following PG device operating frequencies: 4 refers to 433MHz, 8 refers to 868MHz, and 9 refers to 912-919MHz UL/ULC systems.
- HS3032
- HS3128
- HS3248
- HS2LCDPRO
- HS2LCDRFPROx
- HS2LCDWFPROx
- HS2LCDWFVPROx

- HS2TCHPRO
- HS2TCHPROBLK

Securing the premises

The PowerSeries Pro provides multiple arming modes as described below:

Away Mode	Use this mode when there is nobody on the premises. Away mode activates all perimeter and interior sensors in the alarm system.
Stay Mode	Use this mode when someone is on the premises. Stay mode partially activates the alarm system by arming all perimeter sensors and bypassing all interior sensors.
Night Mode	Use when the perimeter and interior need to be armed but require limited movement without activating the alarm (e.g., disable motion sensors in an area containing a washroom). Night mode is similar to Stay mode but only bypasses internal sensors configured as Night Zones.

- ① **Note:** Verify with the alarm company which modes are available. For SIA FAR listed panels, the Stay arming Exit Delay will be twice as long as the Away arming Exit Delay.

Depending on the system configuration, there are multiple methods to arm the system.

Arm the system using a:

- Keypad
- Wireless Key
- Proximity Tag

Arming the system

You can arm the PowerSeries Pro system using a keypad, a wireless key, a proximity tag, or the interactive partner portal.

- ① **Note:** If your system is installed in accordance with SIA CP-01 Standard for False Alarm Reduction, the security system arms in Stay Arm mode if the exit delay time expires and no one has exited the premises.

Arming the system in Away mode using a keypad

Away mode activates the complete alarm system by:

- Arming all perimeter sensors.
- Arming all interior sensors.

Arming the system in Away mode

To arm the system in Away mode, complete the following steps:

1. Ensure that you close all windows and doors.
2. Ensure that the Ready indicator is on.
① **Note:** You cannot arm the system until the Ready indicator is on.
3. Choose one of the following options:
 - To quickly arm the system, press [*][0].
 - To arm the system using the Away key, press and hold the Away key for 2 seconds. If it is necessary, enter an access code, or present a proximity tag to the keypad reader.

If the system bypasses a zone, a warning appears on the keypad.

- ① **Note:** For European installations (EN50131 certified), you can not arm the system without a valid user code. If you do not have a valid user code, do not attempt to initiate the arm sequence for the alarm system.

After you initiate the arming sequence, the system completes the following actions:

- The Armed indicator turns on.
 - The Ready indicator remains lit.
 - The Exit Delay time begins to count down.
 - The keypad beeps six times, and continues to beep once each second. In the final 10 seconds, the system beeps rapidly.
- ① **Note:** For European installations (EN50131 certified), the Armed indicator turns on only after the Exit Delay.

When the Exit Delay timer expires, the system is Armed and the following actions occur:

- The Ready indicator turns off.
 - The Armed indicator remains on.
 - The keypad stops sounding.
- ① **Note:** The installer configures the Exit Delay timer in accordance with the North American and European certification requirements (UL, ULC, and EN50131).

Canceling the arming sequence

To cancel the arming sequence, complete the following step:

- Enter your access code, or present a proximity tag to the keypad reader.

Arming the system in Stay mode

Stay mode partially activates the alarm system by arming all perimeter sensors, and bypassing all interior sensors.

- ① **Note:** For European installations (EN50131 certified), the Keypad Blanking feature activates after 30 seconds. You can see the status of the alarm system only after you enter a valid user code.

To arm the system in Stay mode, complete the following steps:

1. Ensure that you close all windows and doors.
2. Ensure that the Ready indicator is on.
3. Press and hold the Stay key for 2 seconds. If it is necessary, enter an access code, or present a proximity tag to the keypad reader.

- ① **Note:** Do not leave the premises.

If the system bypasses a zone, a warning appears on the keypad.

After you initiate the arm sequence, the system completes the following actions:

- The Armed indicator turns on.
 - The Ready indicator remains lit.
 - The Exit Delay timer begins counting down.
- ① **Note:** For European installations (EN50131 certified), the Armed indicator turns on only after the Exit Delay.

When the Exit Delay timer expires, the system is Armed and the following actions occur:

- The Ready indicator remains lit.

- The Armed indicator remains on.
- The keypad stops sounding.

Canceling the arming sequence

To cancel the arming sequence, complete the following step:

- Enter your access code, or present a proximity tag to the keypad reader.

Silent exit delay

If you arm the system using the Stay key or the No-Entry Arming method [*] [9]:

- The warning beep is silenced
- The exit time doubles only for that exit period (CP-01 versions only).

ⓘ **Note:** For non CP-01 versions, Standard Exit Time is used.

Arming the system with a wireless key

If configured, the PowerSeries Pro system can be armed using the wireless keys provided with your alarm system. To arm the system with a wireless key, press the desired arming mode button when the system Ready indicator is on.

Arming the system with a proximity tag

Proximity tags can be used to arm and disarm the system or to perform a programmed function (e.g. used in place of entering an access code or to unlock a storage room door).

To arm the system with a proximity tag

- Present your proximity tag to a keypad with a proximity sensor when the system Ready indicator is on.
- If configured by your installer, enter your access code.

ⓘ **Note:** When arming with a proximity tag, the system arms in Away mode if you exit the premises. The system arms in Stay mode if a motion sensor is installed and you don't exit the premises.

Night arming

Night mode partially activates the alarm system by:

- Bypassing all internal sensors configured as Night zones.
- Arming all perimeter sensors.
- Arming all other internal sensors.

Arming the system in Night mode is possible after the system has first been armed in Stay mode and [*][1] is pressed at the keypad. The keypad can also be configured with a function key to arm the system in Night Mode. To access armed interior areas when the system is armed in Night Mode, you must disarm the system.

ⓘ **Note:** Ensure that your installer has provided you with a list identifying all programmed night zones. Your installer can configure a function key to arm the panel in Night mode without the system already being armed in Stay mode.

Arming the system in Night mode

To arm the system in Night mode, complete the following steps:

If the system is configured, press and hold the Night Arm key for 2 seconds.

1. After you arm the system in Stay mode, press [*] [*] on any keypad, or press [*] [1].

If it is necessary, enter an access code or present a proximity tag to the keypad reader.

ⓘ **Note:** The system arms all interior zones, except for devices that you program as Night Zones.

Disarming a system that is in Night mode

To disarm a system that is in Night mode, complete the following step:

- Enter your access code.

To gain access to interior areas that are armed during Night mode disarm the system by entering your access code.

No-entry arming

The No-entry feature arms the system in Stay mode and completes the following actions:

- Removes the Entry Delay from configured zones.
- arms all perimeter sensors.
- Bypasses all interior sensors.

ⓘ **Note:** When you use the No-entry feature, an attempt to enter through a door or window creates an instant alarm.

Arming the system using the No-entry arm feature

To arm the system using the No-entry arm feature, complete the following steps:

1. Ensure that the Ready indicator is on, and that the system is ready for Arming .
2. Press [*] [9]. If it is necessary, enter an access code, or present a proximity tag to the keypad reader.

If the system bypasses a zone, a warning message appears on the keypad.

After you initiate the arm sequence, the system completes the following actions:

- The system flashes and has no entry delay.
- The keypad sounds with a fast beep.
- The system displays Exit Delay in Progress on the keypad.

When the Exit Delay timer expires, the system is armed.

Canceling the arm sequence

To cancel the arm sequence, complete the following step:

- Enter your access code, or present a proximity tag to the keypad reader.

Exit Delay Time Restart

This option restarts the exit delay timer if an entry/exit zone is tripped a second time before the end of the exit delay. The exit delay timer can only be restarted once.

The Quick Exit feature

Use the Quick Exit feature if the system is already armed and you would like to leave without disarming and rearming the system. Quick Exit uses the same hot keys as Quick arming, and it provides you with a 2-minute exit delay to leave the premises without triggering an alarm. Once the door you leave from closes, the quick exit timer will be canceled.

Exiting the premises using the Quick Exit feature

To exit a premises using the Quick Exit feature, complete the following steps:

1. If the system is Armed and the Armed light is on, choose one of the following options:
 - Press and hold the Quick Exit key for 2 seconds.
 - Press [*] [0].
2. Exit the premises before the Exit Delay timer expires.

Bypassing zones

⚠ WARNING: If a zone is not operating properly, contact the installer immediately.

Bypassing zones intentionally unprotects specified zones the next time your system is armed. Depending on the type of keypad, bypassed zones will be identified differently. Using an HS2LCD series keypad, bypassed zones are indicated on the LCD screen as shown in the following table.

ⓘ Note: For UL listed installations, zones can only be bypassed manually.

Table 3: LCD Keypad Zone Indications

LCD Display	Indication	Description
Zone Label <>	none	Zone is ready for arming.
Zone Label <> O	O	Zone is currently open. You may be unable to Arm the system.
Zone Label <> B	B	Zone is bypassed.

Bypassed zones:

- Must be configured before arming the system.
- Can be configured using a keypad.
- Allow for access to protected areas when the system is armed.
- Allow you to Arm the system if a zone is temporarily out of service.
- Reduce the level of security.
- Will not sound an alarm.
- Are automatically cancelled each time the system is disarmed.
- Can be programmed together within bypass groups. For more information see "Bypass Groups".

Additional bypass features

Recall Last Bypass	Recalls all zones that were bypassed the last time the bypass zone feature was used.
Bypass All Open Zones	Allows the user to quickly bypass all open zones with a single command.
Clear Bypass	Instantly clears all bypass conditions from the zones assigned to the partition.
Programming a Bypass Group	Use when you consistently bypass the same zones. This feature allows you to store in memory one group of bypassed zones per partition.
Activating a Bypass Group	Loads a stored bypass group from memory.

- ① **Note:** Ensure that no zones are unintentionally bypassed when arming the system.
- ① **Note:** 24-hour zones can only be unbypassed manually.
- ① **Note:** For security reasons, your installer has programmed the system to prevent you from bypassing certain zones (e.g., smoke detectors). For more information on fire zones see “Fire and CO Zone Types”.

Bypassing individual zones

To bypass individual zones, complete the following steps:

1. On the keypad, press [*] [1].
2. **Optional:** If it is necessary, enter an access code, or present a proximity tag.
3. To bypass a zone, choose one of the following options:
 - Enter a three digit zone number.
 - Use the [<] [>] keys to scroll to the zone, and press [*].
4. **Optional:** To toggle or undo the bypassing of a zone, enter the three digit zone number, or press [*].
5. To exit Bypassing mode, press [*].

If the system is ready to arm , the Ready indicator is on.

Bypassing all open zones

To bypass all open zones, complete the following steps:

1. On the keypad, press [*] [1].
2. **Optional:** If it is necessary, enter an access code, or present a proximity tag.
3. Choose one of the following options:
 - Press [9] [9] [8].
 - Use the [<] [>] keys to scroll to Bypass Options, and press [*].
 - Use the [<][>] keys to scroll to Bypass Open Zones, and press [*]
4. To exit Bypassing mode, press [*].

If the system is ready to arm , the Ready indicator is lit.

Recalling the last bypassed zones

To recall the last bypassed zones, complete the following steps:

1. On the keypad, press [*] [1].
2. **Optional:** If it is necessary, enter an access code, or present a proximity tag to the keypad reader.
3. Choose one of the following options:
 - Press [9] [9] [9].
 - Use the [<][>] keys to scroll to Bypass Options, and press [*].
 - Use the [<][>] keys to scroll to Bypass Recall, and press [*]
4. To exit Bypassing mode, press [*].

If the system is ready to arm, the Ready indicator is on.

Clearing the bypass indication from all zones

To clear the Bypass Indication from all zones, complete the following steps:

1. On the keypad, press [*] [1].
2. **Optional:** If it is necessary, enter an access code, or present a proximity tag to the keypad reader.
3. Choose one of the following options:
 - Press [0] [0] [0].
 - Use the [<] [>] keys to scroll to Clear Bypasses, and press [*].
4. To exit Bypassing mode, press [*].

Bypass groups

Program frequently bypassed zones into the system as a bypass group. Using bypass groups avoids individually bypassing each zone. One bypass group can be programmed per partition.

ⓘ **Note:** This feature is not to be used in UL listed installations.

Programming a bypass group

To program a Bypass group, complete the following steps:

1. On the keypad, press [*] [1].
2. **Optional:** If it is necessary, enter an access code or present a proximity tag to the keypad reader.
3. Choose one of the following options:
 - Enter the three digit zone number of the zones you want to bypass.
 - Scroll to the zone you want to bypass and press [*]
4. Choose one of the following options:
 - To program the bypass group with the current bypassed zones, press [9] [9] [5].

- Use the [<] [>] keys to scroll to Bypass Options and press [*], and scroll to Program Bypass Group and press [*].

5. To exit Bypassing mode, press [#].

Loading a bypass group

To load a Bypass group, complete the following steps:

1. On the keypad, press [*] [1].
2. **Optional:** If it is necessary, enter an access code or present a proximity tag.
3. Choose one of the following options:
 - Press [9] [9] [1], and if it is necessary, enter an access code or present a proximity tag.
 - Use the [<] [>] keys to scroll to Bypass Options and press [*], and scroll to Bypass Group and press [*].
4. To exit Bypassing mode, press [#].

Arming troubles and exit faults

Arming troubles

An error tone (long beep) sounds if the system is unable to arm. Arming trouble may occur in the following circumstances:

- The system is not ready to Arm (i.e., sensors are open).
- An incorrect user code is entered.
- A trouble is present and has not been viewed by the user. This operation must be enabled by the installer.

Correcting an arming error

1. Ensure all sensors are secure. Your keypad will identify any open sensors.
2. When the trouble light is on, enter [*][2] and enter [99] or scroll to the Acknowledge All Troubles prompt and press [*]. If your system has been programmed to prevent arming when a trouble is present.
3. Try arming the system again.
4. If troubles persist contact your installer.

Audible exit faults

ⓘ **Note:** This option must be enabled by your installer.

In an attempt to reduce false alarms, the Audible Exit Fault notifies you of an improper exit when arming the system. Improper exits are caused by failing to securely close the Exit/Entry door.

Improper exits cause the following system notifications:

- The keypad emits one continuous beep.
- The bell or siren sounds for the duration of the entry delay until a valid user code is entered or until the programmed Bell Time Out expires.

Correcting an exit fault

1. Re-enter the premises.
2. Disarm the system before the entry delay timer expires by entering your access code, or using a proximity tag, or wireless key.
3. Follow the Away arming procedure again, making sure to close the entry/exit door properly. For more details see: "Away arming the System with the Keypad".

Disarming the system

Depending on your system configuration, there are multiple methods you can use to disarm your system. You can disarm the system using a keypad, a wireless key, or a proximity tag:

Disarming the system with a keypad

- ⓘ **Note:** When you enter the premises, the keypad sounds. To avoid an alarm condition, you must disarm the system within a specific number of seconds.

To disarm the system with a keypad, complete the following step:

- Enter your access code, or present a proximity tag to the keypad reader.

Disarming the system with a wireless key

- ⓘ **Note:** When you enter the premises, the keypad sounds. To avoid an alarm condition, you must disarm the system within a specific number of seconds.

To disarm the system with a wireless key, complete the following step:

- When the system is armed, and the Armed indicator is on, press the disarm key.
- ⓘ **Note:** After you disarm a system with a keypad using a wireless key, ensure that you check the alarm memory to determine if any alarms occurred during the armed period.

Disarming the system with a proximity tag

- ⓘ **Note:** When you enter the premises, the keypad sounds and indicates entry delay. To avoid an alarm condition, you must disarm the system within a specific number of seconds.

To disarm the system with a proximity tag, complete the following step:

- When the system is armed, and the Armed indicator is on, present a proximity tag to the proximity sensor on the keypad.
- ⓘ **Note:** The installer programs the Duration of Entry timer, and advises on the duration of the timer. Valid entries are between 30 seconds and 4 minutes. For SIA CP-01 classified installations, the entry delay must not exceed 45 seconds.

Disarming error

If your code is invalid, the system does not disarm and a 2-second error tone sounds. If this occurs, press [#] and re-enter your access code.

Alarms

The system can generate different alarm sounds, each with a different purpose and priority.

Priority	Type of Alarm	What you hear
1	Fire	Temporal (3 beeps then a pause) or pulsed siren (continuous beeping)
2	Carbon Monoxide	4 beeps, 5 second pause, 4 beeps
3	Intrusion (Burglary)	Continuous siren
4	Flood	1 second on, 3 seconds off, repeating

Using emergency keys

► **Important:** Use only in an emergency.




If you press both the emergency keys you generate a fire, medical, or panic alarm, and you alert the monitoring station. To generate a fire, medical, or panic alarm, complete the following step:

- Press both alarm keys simultaneously for two seconds.

The keypad beeps to indicate that the alarm input is accepted and that an alert is sent to the monitoring station.

ⓘ **Note:** The keypad does not beep for the Panic or Medical alarms

Table 4: Emergency keys

Name	Key
Fire alarm	
Medical alarm	
Panic alarm	

Verify with your alarm company that your system is equipped with emergency keys. Having an optional audio verification module installed on your system allows the monitoring station to open communication when notified of an alarm.

ⓘ **Note:** Fire keys can be disabled by the installer.

Fire alarm

⚠ **WARNING:** If the fire alarm sounds, follow your emergency evacuation plan immediately.

Silencing a fire alarm

If the fire alarm accidentally activates you can silence the alarm. To silence the alarm, complete the following steps:

1. On the keypad, enter your access code.
2. Call your central station to avoid a fire dispatch.

Bells Silenced LCD display for fire alarms

If you silence a fire alarm by entering a user code, and the zone that initiated the fire alarm remains open, a Bells Silenced message displays. The system automatically clears the message when all the

fire zones are restored on the system. When the Bells Silenced message displays, a user can still view all standard base menu messages by using the manual Scroll button.

- ① **Note:** The Bells Silenced message also overrides the automatic display of the Alarm Memory feature for fire alarms.

Resetting smoke detectors

After an alarm condition, reset smoke detectors to exit the alarm condition.

- ① **Note:** Verify with your alarm company if this function is required on your system.

To reset the sensors

1. Press and hold the Reset key on the keypad for 2 seconds. If the reset is successful, the alarm is cancelled.
2. If a smoke detector fails to reset, it may still be detecting an alarm condition. If unsuccessful, the alarm will reactivate or continue. Contact your alarm system provider.

Carbon monoxide alarm

- ⚠ **WARNING:** Carefully review your Carbon Monoxide Alarm Installation/User Guide to determine the necessary actions required to ensure your safety and ensure that the equipment is operating correctly. Incorporate the steps outlined in the guide into your evacuation plan.

Activation of your CO alarm indicates the presence of carbon monoxide (CO), which can be fatal. During an alarm:

- The red LED on the CO detector flashes rapidly and buzzer sounds with a repeating cadence of 4 quick beeps, 5-second pause, 4 quick beeps.
- The siren connected to the control panel produces the same cadence as above.
- The keypad provides audible and visual indication of the CO alarm.

If the Carbon Monoxide Alarm Sounds

1. Immediately move outdoors or to an open door/window.
2. Call emergency services or your fire department.

Bells Silenced LCD display for CO alarms

If you silence a CO alarm by entering a user code, and the zone that initiated the CO alarm remains open, a Bells Silenced message displays. The system automatically clears the message when all the CO zones are restored on the system. When the Bells Silenced message displays, a user can still view all standard base menu messages by using the manual Scroll button.

- ① **Note:** The Bells Silenced message also overrides the automatic display of the Alarm Memory feature for CO alarms.

Intrusion and burglary alarm

- ⚠ **WARNING:** If you are unsure of the source of the alarm approach with caution.

The intrusion and burglary alarm is a continuous siren. If the Intrusion alarm was accidental, complete the following steps:

1. Enter your Access Code to silence the alarm. If the code is entered within 30s (or the programmed value of the alarm transmission delay) the transmission of the alarm to the monitoring station will be cancelled.
 - Call your central station to avoid a dispatch.

Alarm Cancel window

The control panel provides a period of time in which the user can cancel the alarm transmission (minimum duration is 5 minutes). If the programmed alarm transmission delay has expired, canceling an alarm sends a message to the monitoring station. Upon a successful transmission of the cancellation message, the keypad beeps 6 times. Must be enabled and configured by the installer.

ⓘ **Note:** For CP-01 systems, alarm transmission delay must not exceed 45 seconds.

Viewing alarms in memory

When an alarm occurs the keypad indicator illuminates. Viewing the Alarm Memory provides more information on the sensor(s) that were activated.

To View Alarms in Memory

Press [*][3] or use the scroll keys to navigate to Alarm Memory and press [*].

Alarm messages

LCD	What it means
Burglary Verified	Multiple burglary sensors were activated. Central station has been notified.
Burglary Not Verified	A single burglary sensor was activated. Central station has been notified.
Hold-up Verified	Multiple hold-up sensors were activated. Central station has been notified.
Hold-up Not Verified	A single hold-up sensor was activated.
Fire Alarm	Fire alarm has been triggered. Central station has been notified.
CO Alarm	CO alarm has been triggered. Central station has been notified.

Wireless keys

In addition to the keypad, the PowerSeries Pro system can be controlled using a variety of devices:

- Wireless Keys
- Proximity Tags

Using wireless keys

Wireless keys allow users in close proximity of their premises the ability to readily arm and disarm their system, and to call for help. When using compatible wireless keys there is one beep for arming and two beeps for disarming. The wireless key buttons can also be programmed for various functions, including Instant Stay Arm. Check with your installer for details.

ⓘ **Note:** The panic feature has not been evaluated by UL for the PG9929/PG9939.

For additional information, refer to your Wireless Key Instruction Sheet.

Using Proximity Tags

Proximity tags can be used to arm and disarm the system, perform a programmed function and can also be used in place of your user access code.

To operate, present the tag close to the **Tag Reader** icon on your keypad. The LED bar flashes 3 times upon a valid proximity tag being read by the keypad successfully.

ⓘ **Note:** Proximity tags must be enrolled on the system (see "Enrolling and Deleting Proximity Tags").

Managing Users

The maximum number of access codes are as follows:

- 72 for HS3032
- 1000 for HS3128
- 1000 for HS3248

Each user access code can be:

- Uniquely labeled.
- Assigned a proximity tag. In order to operate, proximity tags must be enrolled in the system.
- Assigned to only operate specific partitions. For more information on partitions see: "Managing Partitions".
- Configured with additional attributes. For more information see: "Configuring additional User Options".

❶ **Note:** Your installer configures all access codes to be either 4, 6, or 8 digits.

Access code types

The alarm system provides the following user access code types:

Code	Add user	Delete user	Arm	Disarm	Access codes	User functions	Installer
Master	All	All	Yes	Yes	Yes	Yes	No
User	No	No	Yes	Yes	No	No	No
Supervisor	All but Master	All but Master	Yes	Yes	Yes	Yes	No
Duress	No	No	Yes	Yes	No	No	No
One-time user	No	No	Yes	1/day	No	No	No

Installer and Master codes are system codes that can be changed but not deleted. The other codes are user-defined and can be added or deleted as necessary. By default, access codes have the same partition and attribute programming as the code used to program them.

When using 8-digit access codes, each user can have the following maximum number of unique code variations:

- 1,388,888 for HS3032
- 100,000 for HS3128
- 100,000 for HS3248

The system accepts all codes.

Code type	Description
Master code	By default, the master code can access all partitions and can perform any keypad function. This code can be used to program all access codes, including the supervisor and duress codes. The master code number is [01].
User codes	This type of access code is used to arm and disarm assigned partitions and can access the User Functions menu.
Supervisor codes	Use when you want to allow additional users to manage access codes [*5] or User Functions [*6]. Supervisor codes created by the master code have the same attributes as the master code. Supervisor codes created by another supervisor code have the same attributes, except the supervisor attribute. After creation, attributes can be changed for all supervisor codes. For information on how to program a supervisor code see "Configuring additional User Options".
Duress codes	A Duress Code is used if forced to access your keypad under threat. Duress codes function the same as user access codes, except they transmit a Duress Report to your monitoring station when used to perform any function on the system. Duress codes cannot be used to change Access Codes [*5], User Functions [*6] or Installer [*8] programming. For information on how to program a Duress Code, see "Configuring additional User Options".
One Time user code	Used to grant someone one-time access to your home, i.e., a cleaning person or contractor. The ability to disarm the system is reset at midnight or when the one-time user code is keyed in by the master code user. For information on how to program a One Time User Code, see "Configuring Additional User Options".

Opening the access codes menu

To open the **Access Codes** menu, complete the following steps:

1. On the keypad, press *** 5**.
2. Enter your access code.
3. Choose one of the following options:
 - Enter the user's number, and press *****.
 - Use the **Arrow** keys to navigate through the list of users, and press ***** to select a user.
4. Press **#** to return to the ready state.

Adding, changing, and deleting access codes

Each configured user is assigned a number as follows:

- 01-72 for HS3032
- 01-1000 for HS3128
- 01-1000 for HS3248

A "-" beside a user ID indicates it is not programmed.

Adding or changing a user access code

To add or change a user access code, complete the following steps:

1. On the keypad, press *** 5**.
2. Enter your access code.

3. Choose one of the following options:
 - Use the **Arrow** keys to navigate to the user, and press * *.
 - Enter the user number, and press **.
 - ① **Note:** A dash indicates that there is no user code that corresponds to the user number.
 4. Enter a new four, six, or eight digit access code.
 - ① **Note:** If you enter a duplicate code, the system sounds an error tone.
- When the system programs the new code, a **P** appears and the display reverts to the **Access Codes** menu.

Enrolling a proximity tag

When you enroll or delete proximity tags for a user, there is a choice of options. For more information see [Using Proximity Tags](#).

To enroll a proximity tag, complete the following steps:

1. On the keypad, press * 5.
 2. Enter your access code.
 3. Use the **Arrow** keys to navigate to a user and press *.
 4. Navigate to **Prox Tag**, and press *.
 5. Present the proximity tag to the reader. If the tag enrolls successfully, the blue LED bar flashes, and a **T** appears next to the user's name. For touchscreen keypads, the **Home** button flashes.
- ① **Note:** If a tag is enrolled for another user, or if the tag is invalid, a message displays.

Deleting a proximity tag

To delete a proximity tag, complete the following steps:

1. On the keypad, press * 5.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to a user and press *.
4. Navigate to **Prox Tag**, and press *.
5. Press * to delete the tag.

User labels

You can add a user label using the keypad to give a user a unique name. You can input letters and numbers using the keypad to add or edit user labels. Each number on the keypad corresponds to three letters and one number. Press a number button once, twice, or three times on the keypad to give you a different letter or number. For more information on what letter corresponds to each number on the keypad, see the following table:

Table 5: Keypad numbers and corresponding letters

Keypad button	Corresponding letter and number
1	A, B, C, 1
2	D, E, F, 2
3	G, H, I, 3
4	J, K, L, 4
5	M, N, O, 5
6	P, Q, R, 6
7	S, T, U, 7
8	V, W, X, 8
9	Y, Z, 9
0	0

Adding and editing a user label

To add a user label, complete the following steps:

1. On the keypad, press ***5**.
2. Enter your user access code.
3. Use the **Arrow** keys to navigate to a user label, and press *****.
4. In the **User Codes** menu, navigate to **User Labels** and press *****.
5. Use the number keys to enter a user label, and press *****.

Assigning a partition to a user code

You can configure user codes to give access only to specific partitions. For more information, see [Managing partitions](#).

ⓘ Note: The installer must configure the partitions.

To assign a partition to a user code, complete the following steps:

1. On the keypad, press *** 5**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to the user, and press *****.
4. Navigate to **Partition Assign**, and press *****.
5. Choose one of the following options:
 - To grant the user access to the partition, select **Y**.
 - To deny the user access to the partition, select **N**.

Configuring additional user options

You can also assign users the following additional options:

Table 6: User options

[1] Supervisor Code	For more information see "Access Code Types".
[2] Duress Code	For more information see "Access Code Types".
[3] Zone Bypass	Grants the user the ability to bypass zones.
[7] Bell Squawk	Use to generate a bell squawk when arming and disarming the system.
	i Note: When using wireless keys to arm and disarm the system there will be: <ul style="list-style-type: none">• one bell squawk for arming.• two bell squawks for disarming.• three squawk pairs when disarming with an alarm in memory.
[8] One Time Use	For more information see "Access Code Types".

To configure additional user options, complete the following steps:

1. On the keypad, press * 5.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to the user, and press *.
4. Navigate to **User Options** and press *.
5. Navigate through the options, and press * to select the option you want. For more information, see Table 6.

Accessing the user function menu

The PowerSeries Pro allows for a variety of user configurable functions as listed below:

Event Buffer	AutoArm Time	Late To Open	Contrast Control	User's Walk Test
Time and Date	System Service/DLS	Late To Open Time	Buzzer Control	AutoArm/Disarm
Voice Chime	User Call-Up	Brightness Control	Voice Prompt	

① **Note:** You can modify user functions only when the system is disarmed.

To access the **User Function** menu, complete the following steps:

1. On the keypad, press * **6**.
2. Enter your access code.
3. Press # to return to the ready state.

Viewing the event buffer

The event buffer displays a list of the last 500 events on the HS3032, and the last 1000 events on the HS3128/HS3248. You can only view the event buffer using an LCD keypad.

To view the event buffer, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Event Buffer**, and press *****.
4. Use the **Arrow** keys to scroll through the events.

Setting the time and date

To set the time and date, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Time and Date**, and press *****.
4. Use the number keys to set the date and time.
5. Press **#** to return to the ready state.

Configuring the auto arm and disarm feature

① **Note:** The installer must configure this feature.

To configure the auto arm and disarm feature, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Auto Arm/Disarm**, and press *****.
4. Press ***** to enable or disable the feature.

Setting the auto arm time

You can configure the system to auto arm at a specific time on each day of the week. If you do not configure a specific time for a day of the week, the system does not arm automatically on that day.

① **Note:** The installer must configure this feature.

To set the auto arm time, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Auto Arm Time**, and press *****.
4. Navigate to a day of the week, and press *****.
5. Use the number keys to set the time in a 24-hour format.
① **Note:** If you set an invalid time, the keypad sounds an error tone.
6. **Optional:** To set the auto arm time for another day of the week, repeat Steps 4 to 5.

Disabling the auto arm time

To disable the auto arm time, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Auto Arm Time**, and press *****.
4. Navigate to the day of the week and press *****.
5. Enter **9999**.
6. **Optional:** To disable the auto arm time for another day of the week, repeat Steps 4 to 5.

Configuring the system service DLS

Occasionally, your installer may need to remotely access the Installer programming of your security system using Downloading Software (DLS). In order for this to successfully occur, you may need to manually allow access to your system.

① **Note:** The installer must configure the access to this feature.

To configure the system service DLS, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **System Serv/DLS**.
4. Press ***** to enable or disable the feature.
5. Press **#** to return to the ready state.

User Callup

Using DLS, User Call-up allows your system to make one attempt to connect to the installer's remote computer. For a successful connection, the remote computer must be waiting for the system's call.

① **Note:** The installer must configure the access to this feature.

To perform a user callup, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **User Callup**, and press *****. The system attempts to connect to the installer's computer.
4. Press **#** to return to the ready state.

Configuring the late to open feature

The late to open feature provides notification if the alarm system is not disarmed by the programmed time of day.

① **Note:** The installer must configure the access to this feature.

To configure the late to open feature, complete the following steps:

1. On the keypad, press *** 6**.

2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Late to Open**.
4. Press ***** to enable or disable the feature.

Setting the late to open time feature

To set the late to open time feature, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Late to Opn Time**, and press *****.
4. Navigate to the day of the week, and press *****.
5. Use the number keys to set the time in a 24-hour format.
Note: If you set an invalid time, the keypad sounds an error tone.
6. **Optional:** To set the late to open time for another day of the week, repeat Steps 4 to 5.

Disabling the late to open time feature

To disable the late to open time feature, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Late to Opn Time**, and press *****.
4. Navigate to the day of the week and press *****.
5. Enter **9999**.
6. **Optional:** To disable the Late to Open Time feature for another day of the week, complete Steps 4 to 5.

Changing the brightness of the LCD keypad

To change the LCD brightness, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Bright Control**, and press *****.
4. Navigate to the brightness level that you want.
5. Press **#**.

Changing the contrast of the LCD keypad

To change the LCD contrast, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Contrast Control**, and press *****.
4. Navigate to the contrast value that you want.

5. Press # .

Setting the buzzer volume

To set the buzzer volume, complete the following steps:

1. On the keypad, press * 6.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Buzzer Control**, and press *.
4. Navigate to the volume level that you want.
5. Press #.

Setting the voice prompt volume

This feature is available only when using an HS2LCDWFVPRO wireless keypad.

To set the voice prompt volume, complete the following steps:

1. On the keypad, press * 6.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Voice Prompt**, and press *.
4. Navigate to the volume level that you want, and press *.
5. Press # to return to the ready state.

Setting the voice chime volume

This feature is available only when using a HS2LCDWFVPRO wireless keypad.

To set the voice chime volume, complete the following steps:

1. On the keypad, press * 6.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Voice Chime**, and press *.
4. Navigate to the volume level that you want, and press *.
5. Press # to return to the ready state.

Resetting the system

Engineer's reset

If an alarm occurs on your system and the Ready light is off, you cannot rearm your system until you restore the alarm condition or you bypass the opened zone. When you disarm the system after an alarm condition, if **Reset Required** displays on your keypad, contact your installer.

① **Note:** The installer must configure this feature.

Remote (anti-code) reset

When configured by the installer, an alarm condition will cause the system to require a remote reset and arming will no longer be possible after the system is disarmed. This feature ensures that the end user contacts the monitoring station following an alarm condition. The system keypads will display that a remote reset is required and will show a random 5-digit remote reset code. You

must contact the monitoring station and provide the code that's displayed on the keypad. The monitoring station operator will provide a different 5-digit code that the user can enter at the system keypad, which will clear the remote reset condition, allowing the panel to be armed again.

Some user functions are still available while the system is locked out. The user can loan the keypad to a different partition, and can access [*][6] User Functions so the event buffer can be reviewed to determine cause of the alarm condition. The [*][3] Alarms in Memory and [*][7] command output menus are also available during the remote reset condition.

This feature is intended to be used with burglary zones. Fire alarms do not generate remote reset. Each partition will generate a unique Remote Reset code on the system keypads and must be unlocked separately.

Initiating a walk test

This feature allows the user to verify the operation of system detectors and notify the central station that a Walk Test is in progress.

① **Note:** The installer must configure this feature.

➤ **Important:** During a system (walk) test, do not activate any:

- Fire, Auxiliary or Police buttons
- Fire or CO sensors

A full system test is comprised of activating each sensor in turn. Open each door, window and walk in areas with motion detectors. Perform system tests during off-peak hours, such as early morning or late evening. When a test is in progress, the Ready, Trouble and Armed LEDs flash.

To initiate a walk test, complete the following steps:

1. On the keypad, press * 6.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Walk Test**.
4. Press *. The system activates all the keypad sounders, bells, and sirens for two seconds. The system sends a notification to inform the central station that a walk test has started.
5. Trigger each zone or detector by sequence. The keypad sounds, all LEDs on the keypad flash, and the system records the event in the event buffer.
6. Restore the zones.
7. To end the walk test, complete the following steps:
 - a. Press* 6.
 - b. Enter your access code.
 - c. Press 8.

① **Note:** Fire zones, the F key, and 2-wire smoke detectors are excluded from the test. Activation of these zones causes the system to exit the walk test and transmit an alarm condition to the monitoring station.

If you initiate a walk test and do not activate a zone within 15 minutes, the system automatically exits the walk test. The system sounds for 5 minutes before the test ends.

① **Note:** This feature is not available in CP-01 panels.

Canceling a walk test

To cancel a walk test, complete the following steps:

1. On the keypad, press *** 6**.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to **Walk Test**.
4. Press ***** to cancel the test.

Managing partitions

A partition is a limited area of the premises which operates independently from the other areas. Partitioning a system can be beneficial if the property has outbuildings that need to be secured independently of a main area or if the home has a separate apartment. Each partition can have its own keypad, or a keypad can have access to all partitions. User access to partitions is controlled via access code. A master code can access the entire system and partitions, while a user code is limited to assigned partitions.

Partitions

Keypads can be configured to control an individual partition or all partitions.

❶ **Note:** Access to this feature must be configured by installer.

Single partition operation

Single partition keypads provide access to alarm functionality for an assigned partition. Single partition keypads behave as follows:

- Displays the armed state of the partition.
- Displays open zones, if assigned to the partition the keypad is on.
- Displays bypassed zones and allows zone bypassing or creating bypass groups of zones assigned to the keypad partition.
- Displays system troubles (system low battery, system component faults/tampers).
- Displays alarms in memory that occurred on the partition.
- Allows the door chime to be enabled/disabled.
- System test (sounds bells/PGMs assigned to the partition).
- Label programming (zone, partition and user labels for the partition).
- Command output controls (outputs assigned to the partition, or global outputs such as smoke detector reset).
- Temperatures.

Loaning a keypad to another partition

Keypads can be loaned to operate on other partitions (LCD keypads only). When a keypad is loaned from either the global state or from another partition, it may be configured to behave on the loaned partition just as it would if it was originally assigned there.

An access code must be entered before loaning a keypad to another partition. An access code is also required to perform any function on that partition.

To loan a keypad to another partition, complete the following steps:

1. Press and hold **#** for two seconds.
2. Enter your access code.
3. Use the **Arrow** keys to navigate to a partition, and press *****. The keypad is temporarily loaned to this partition. If the keypad is inactive for more than 30 seconds, it reverts to its original partition.

The status of each partition will be identified by a partition flag. For an explanation on partition flags, see the following table.

Table 7: Partition Flags

LCD Display	Flag	Description
1 2 3 4 5 6 7 8 R X A ! E - P N	1-8	Partition number
	R	Partition is ready to be armed
	X	Partition is in exit delay
	A	Partition is armed
	!	Partition is in alarm
	E	Partition is in entry delay
	-	Partition is not configured
	P	Partition auto arm pre-alert
	N	Partition is not ready to be armed

Keypads can also be configured as global keypads, controlling all partitions. Global keypads must be configured by your installer.

Fire and CO zone types

- If a Fire zone generates an alarm only the partition the fire zone is assigned to will go into alarm. Other partitions retain their current state.
- If the [F] key on a global keypad is used to generate an alarm all enabled partitions will go into alarm.
- One or more fire zones may be located on any partition.
- On alarm, the fire auto-scroll display appears on all partition keypads and on all global keypads. Fire alarm silence and fire system reset may be done directly on any partition keypad. To silence a fire or CO alarm from a global keypad requires that the global keypad be loaned to one of the partitions.

Additional features

Viewing a temperature in a zone

This feature displays the temperature for each active zone. To view the temperature in a zone, complete the following steps:

- ① **Note:** An installer must activate this feature.
- 1. On any partitioned keypad, from the Main menu press [*].
- 2. Choose one of the following options:
 - To select a temperature, press [*].
 - For quick access, press [*] [*], and scroll through the menu to view the temperature capable zones.
- 3. To exit, press [#].

Turning the chime on or off

Turning the chime on audibly notifies you when an entry/exit sensor is activated.

To turn the chime on or off, complete the following step:

- Press and hold the **Chime** key.

Audio verification

Allows the monitoring station to initiate an audio (talk/listen) or 1-way audio (listen-in only) session when an alarm has been received. This feature is used to verify the nature of the alarm or determine the type of assistance required by the occupant.

- ① **Note:** This is a supplementary feature that has not been investigated by UL/ULC.
- ① **Note:** Must be enabled and configured by installer.

Visual verification

Allows the monitoring station to use video clips captured from system motion cameras for verification of any alarms.

- ① **Note:** This is a supplementary feature that has not been investigated by UL/ULC.
- ① **Note:** Must be enabled and configured by installer.

Video on demand

The video on demand feature uses third-party integrations to obtain video clips on demand from the connected cameras.

- ① **Note:** The installer must configure and activate this feature.

PIR camera zone association

The PowerSeries Pro system can link up to eight zones to any passive infrared (PIR) camera that connects to the system. When a zone goes into alarm, the PIR camera can trigger a video capture so that a user can verify the alarm.

① **Note:** The installer must configure and activate this feature.

Activating a command output

While being useful for many applications, Command outputs are typically configured to operate items such as garage doors or electric gates. Additionally, command outputs can be assigned to follow a schedule configured by your installer.

This is a supplementary feature that has not been investigated by UL/ULC.

Must be configured by installer.

To activate a command output, complete the following steps:

1. On the keypad, press *** 7**.
2. Use the **Arrow** keys to navigate to the output control option you want, and press *****.
3. Enter your access code to activate the command output.

Configuring a command output to follow a schedule

To configure a command output to follow a schedule, complete the following steps:

1. On the keypad, press *** 7**.
2. Use the **Arrow** keys to navigate to the follow schedule option, and press *****.
3. Enter your access code or present a proximity tag.
4. Navigate to the command output that you want, and press *****.

Burglary verification

The PowerSeries Pro system includes cross zone and sequential detection features that require an activation on two or more zones, within a given time period, to generate a confirmed alarm and immediate police response.

① **Note:** This feature must be enabled and configured by your installer.

Call waiting

The PowerSeries Pro system includes a programmable option for call waiting to prevent a call waiting line from interfering with the alarm verification process. This option is disabled by default.

① **Note:** This feature must be enabled and configured by your installer.

Fire alarm verification

Fire Alarm Verification is an available option for Fire zones. If configured, and the conditions for alarm verification are met, the fire alarm sounds and an alarm transmission is sent to the monitoring station.

① **Note:** This feature must be enabled and configured by your installer.

System lockout due to invalid attempts

If too many invalid access codes are entered, your system can be configured to automatically lockout input from all keypads, wireless keys and proximity tags for a programmed duration. If this happens, wait the programmed duration then try again.

- ① **Note:** This feature and lockout duration must be configured by your installer. Fire, Medical and Panic keys are still active during a System Lockout.

Troubleshooting

Occasionally, you may have a problem with your Alarm Controller or telephone line. If this happens, your Alarm Controller will identify the problem and display an error message. Refer to the provided list when you see an error message on the display. If additional help is required, contact your distributor for service.

- ① **Note:** There are no parts replaceable by the end-user within this equipment, except for the keypad batteries. Dispose of used batteries as per local rules and regulations.

Trouble conditions

When a trouble condition occurs your Alarm System identifies the problem and displays an error message. Refer to the table below when you see an error message on the display. If additional help is required, contact your distributor for service.

When the system detects a trouble condition the following occurs:

- The Trouble indicator turns on.
- The keypad beeps twice every 10 seconds. Press the [*] key to silence the keypad beeps.

Press [*][2] to examine troubles. When viewing troubles, the trouble indicator flashes to identify the level of trouble being viewed. One flash = level 1, two flashes = level 2 etc. Arming of your system may be impeded by a trouble. To override this condition, enter [*][2], scroll to Acknowledge All Troubles and press [*] or enter 999.

Table 8: Trouble conditions

Trouble Condition	Trouble Level 1	Description	Trouble Types	Trouble Level 2	Notification Level 3
Trouble numbers are used to view the trouble. Trouble Notification identifies the range that may be displayed on the keypad. When exploring the trouble levels, the Trouble indicator will flash to identify which level you are currently viewing.					
Service Required	01	Assorted Trouble types. Time and Date troubles can be resolved by resetting the Time/Date. To set Time/Date press [*][6][0][1]. For all other troubles call for service.	Bell Circuit	01	
			RF Jam	02	
			Loss of clock	04	
			Output 1 Fault	05	
			Warm Start	06	
			USB Wi-Fi Connected	07	
			Component fault in power unit	08	
			Power Fail Bus Repeater	09	Repeater 1-16
			Power Fail 3A Supply	10	Power Supply 1-4
			Overcurrent	11	Call for service

Table 8: Trouble conditions

Trouble Condition	Trouble Level 1	Description	Trouble Types	Trouble Level 2	Notification Level 3
Battery Trouble	02	The system has detected a battery trouble condition. Call for service.	Low Battery	01	n/a
			No Battery	02	n/a
			Low Battery	04	Module 1-4
			High-current O/P		
			No Battery	05	Module 1-4
			High-current O/P		
			Low Battery	07	Module 1-4
			1A Power Supply		
			No Battery	08	Power supply 1-4
			1A Power Supply		
			Low Battery Bus Repeater	10	Repeater 1-16
			No Battery Bus Repeater	11	Repeater 1-16
			Low Battery 1 3A Power Supply	13	Power Supply 1-4
			Low Battery 2 3A Power Supply	14	Power Supply 1-4
No Battery 1 3A Power Supply	15	Power Supply 1-4			
No Battery 2 3A Power Supply	16	Power Supply 1-4			
Bus Voltage	03	A module has detected a low voltage on its corbus red terminal.	HSM2HOST	01	n/a
			Keypad	02	Keypad 1-32
			Zone Expander	04	Zone expander 1-30
			1A Power Supply	05	Power Module 1-4
			High-current Output	06	Output Module 1-4
			System Area	07	n/a
			Output Expander	08	Module 1-16
			Audio Module	09	n/a
			8 I/O Module	10	Module 1-30
			Bus Repeater	11	Repeater 1-16
			Bus Fault	12	Repeater 1-16
			Bus Repeater		
			3A Power Supply	13	Power Supply 1-4
AC Troubles	04	The system is experiencing loss of power. Call for service. If the building and/or neighborhood has lost electrical power, the system will continue to operate on battery for several hours.	Zone	01	Zone label or 001-248
			Keypad	02	Keypad 1-32
			Siren	03	Siren 1-16
			Repeater	04	Repeater 1-8
			Power Supply	05	Power supply 1-4
			High-current Output	06	Output terminal 1-4
			System Area	07	n/a
			Bus Repeater	08	Repeater 1-16
			3A Power Supply	09	Power Supply 1-4

Table 8: Trouble conditions

Trouble Condition	Trouble Level 1	Description	Trouble Types	Trouble Level 2	Notification Level 3
Device Faults	05	The system has detected an issue with one or more connected devices. Call for service.	Zone	01	Zone label or 001-248
			Keypad	02	Keypad 1-32
			Siren	03	Siren 1-16
			Repeater	04	Repeater 1-8
			Device Mask	06	Zone 001-248
			Gas	07	Zone 001-248
			Heat	08	Zone 001-248
			CO	09	Zone 001-248
			Freeze	10	Zone 001-248
			Probe Disconnected	11	Zone 001-248
			Fire	12	Zone 001-248
			Device Battery	06	The system detected an issue with one or more device batteries. For zone, keypad and wireless key battery troubles see the accompanying documentation for how to change the batteries.
Keypad	02	Keypad 1-16			
Siren	03	Siren 1-16			
Repeater	04	Repeater 1-8			
User	05	Wireless key 1-32			
Device Tamperers	07	The system has detected a tamper condition with one or more devices on the system. Call for service.	Zone	01	Zone label or 001-248
			Keypad	02	Keypad 1-32
			Siren	03	Siren 1-16
			Repeater	04	Repeater 1-8
			Audio Station	05	Station 1-4
RF Delinquency	08	The system has detected wireless signal interference that is causing improper system operation. Call for service.	Zones	01	Zone label or 001-248
			Keypad	02	Keypad 1-16
			Siren	03	Siren 1-16
			Repeater	04	Repeater 1-8
Module Supervision	09	The system has detected a supervisory trouble condition with one or more modules on the system. Call for service.	HSM2HOST	01	n/a
			Keypad	02	Keypad 1-32
			Zone Expander	04	Expander 1-30
			Power Supply	05	Power Supply 1-4
			High-current Output	06	Output terminal 1-4
			Output Expander	08	Output module 1-16
			Audio Module	09	
			I/O Module	10	Module 1-30
			Bus Repeater	11	Repeater 1-16
			3A Supply	12	Power Supply 1-4

Table 8: Trouble conditions

Trouble Condition	Trouble Level 1	Description	Trouble Types	Trouble Level 2	Notification Level 3
Module Tamperers	10	The system has detected a tamper condition with one or more modules on the system. Call for service.	HSM2HOST	01	n/a
			Keypad	02	Keypad 1-32
			Zone Expander	04	Zone Expander 1-30
			Power Supply	05	Power Supply 1-4
			High-current Output	06	Output terminal 1-4
			Output Expander	08	Output module 1-16
			Audio Module	09	n/a
			I/O Module	10	Module 1-30
			Bus Repeater	11	Repeater 1-16
Communications	11	The system has detected a communication trouble. Call for service.	3A Power Supply	12	Power Supply 1-4
			Telephone line monitoring	01	n/a
			Failure to communicate	02	Receiver 1-4
			SIM Lock	03	n/a
			Cellular	04	n/a
			Ethernet	05	n/a
			Receiver	06	Receiver 1-4
			Supervision Receiver	07	Receiver 1-4
			Alt Comm Fault	09	n/a
Alt Comm FTC	10	Receiver 1-4			
Not Networked	12	The system has detected a network trouble condition with one or more modules on the system. If the trouble does not restore within 20 minutes, call for service.	Zone	01	Zone label 001-248
			Keypad	02	Keypad 1-32
			Siren	03	Siren 1-16
			Repeater	04	Repeater 1-8
			User	05	Users 01-1000
AUX Trouble	13	The system has detected a trouble on the AUX terminal.	Zone	01	Zone
			Power Supply	05	Power Supply 1-8
			High-current O/P	06	Module 1-4
			System Area	07	n/a
			8 I/O Module	10	Module 1-30
			Bus Repeater	11	Repeater 1-8
			3A Power Supply Aux 1	12	Aux 1 Trouble
			3A Power Supply Aux 2	13	Aux 2 Trouble
Limited Exceeded	14	The system detects incompatibility with third-party firmware.	Interactive zone limit	01	n/a
			Interactive partition limit	02	n/a

Reference sheets

Fill out the following information for future reference and store this guide in a safe place.

System information

- o [F] FIRE
- o [M] MEDICAL
- o [P] PANIC



The Exit Delay Time is _____ seconds.



The Entry Delay Time is _____ seconds.

Service contact information

Central Station Information

Account #: _____ Telephone #: _____

Installer Information

Company: _____ Telephone #: _____

Battery Installation / Service Date:

- **Important:** If you suspect a false alarm signal has been sent to the central monitoring station, call the station to avoid an unnecessary response.

Access codes

Master Code [01] : _____

User	Access code	User	Access code	User	Access code	User	Access code

ⓘ **Note:** Copy this page as needed to record additional access codes.

Sensor and zone information

Zone	Protected area	Sensor type	Zone	Protected area	Sensor type

① **Note:** Copy this page as needed to record additional zone information.

Locating detectors and escape plan

The following information is for general guidance only and it is recommended that local fire codes and regulations be consulted when locating and installing smoke and CO alarms.

Smoke detectors

Research has shown that all hostile fires generate smoke to a greater or lesser extent. Experiments with typical fires in homes indicate that detectable quantities of smoke precede detectable levels of heat in most cases. For these reasons, smoke alarms should be installed outside of each sleeping area and on each storey of the home.

The following information is for general guidance only and it is recommended that local fire codes and regulations be consulted when locating and installing smoke alarms.

It is recommended that additional smoke alarms beyond those required for minimum protection be installed. Additional areas that should be protected include: the basement; bedrooms, especially where smokers sleep; dining rooms; furnace and utility rooms; and any hallways not protected by the required units. On smooth ceilings, detectors may be spaced 9.1 m (30 feet) apart as a guide. Other spacing may be required depending on ceiling height, air movement, the presence of joists, uninsulated ceilings, etc. Consult National Fire Alarm Code NFPA 72, CAN/ULC-S553-02 or other appropriate national standards for installation recommendations.

- Do not locate smoke detectors at the top of peaked or gabled ceilings; the dead air space in these locations may prevent the unit from detecting smoke.
- Avoid areas with turbulent air flow, such as near doors, fans or windows. Rapid air movement around the detector may prevent smoke from entering the unit.
- Do not locate detectors in areas of high humidity.
- Do not locate detectors in areas where the temperature rises above 38°C (100°F) or falls below 5°C (41°F).
- Smoke detectors must always be installed in USA in accordance with Chapter 29 of NFPA 72, the National Fire Alarm Code: 29.5.1.1.

Where required by applicable laws, codes, or standards for a specific type of occupancy, approved single- and multiple-station smoke alarms shall be installed as follows:

1. In all sleeping rooms and guest rooms.
2. Outside of each separate dwelling unit sleeping area, within 6.4 m (21 ft) of any door to a sleeping room, the distance measured along a path of travel.
3. On every level of a dwelling unit, including basements.
4. On every level of a residential board and care occupancy (small facility), including basements and excluding crawl spaces and unfinished attics.
5. In the living area(s) of a guest suite.
6. In the living area(s) of a residential board and care occupancy (small facility).



Figure 1

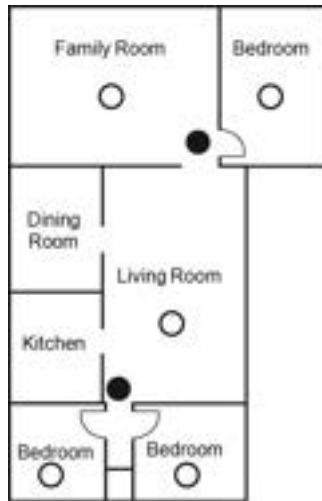


Figure 2

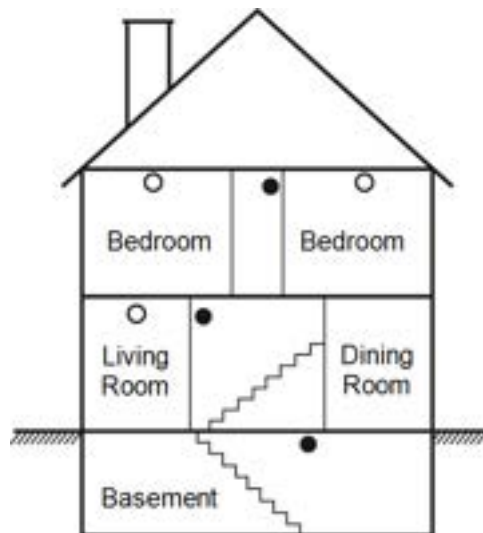


Figure 3

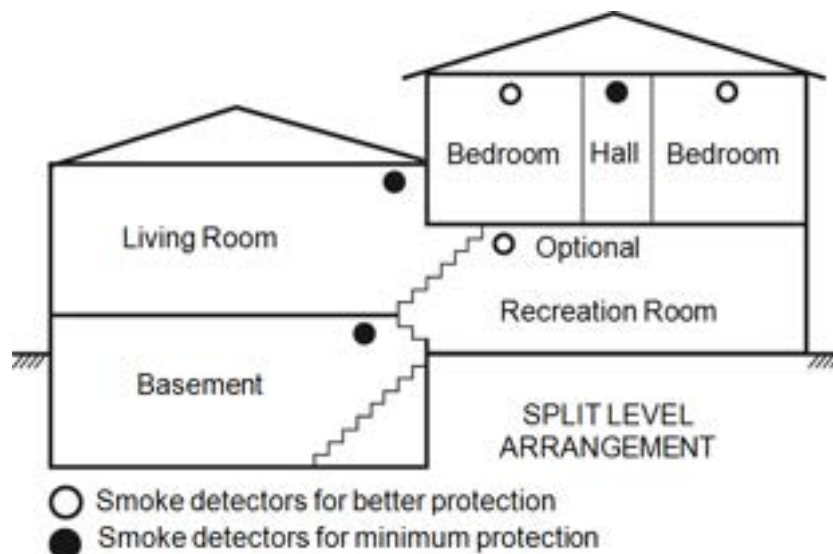


Figure 3a

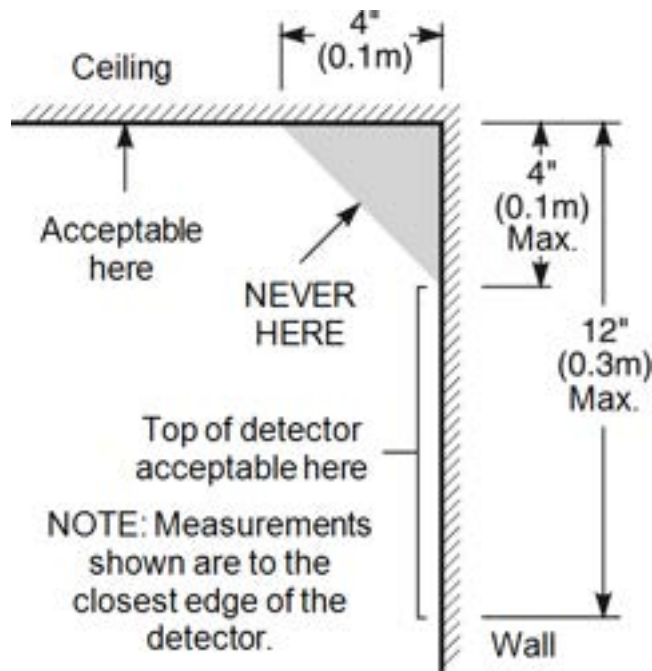


Figure 4

Fire escape planning

There is often very little time between the detection of a fire and the time it becomes deadly. It is very important that an emergency escape plan be developed and rehearsed.

- Study the possible escape routes from each location within the house. Since many fires occur at night, special attention should be given to the escape routes from sleeping quarters.
- Escape from a bedroom must be possible without opening the interior door.

Consider the following when making your escape plans:

- Make sure that all border doors and windows are easily opened. Ensure that they are not painted shut, and that their locking mechanisms operate smoothly.

- If opening or using the exit is too difficult for children, the elderly or handicapped, plans for rescue should be developed. This includes making sure that those who are to perform the rescue can promptly hear the fire warning signal.
- If the exit is above the ground level, an approved fire ladder or rope should be provided as well as training in its use.
- Exits on the ground level should be kept clear. Be sure to remove snow from exterior patio doors in winter; outdoor furniture or equipment should not block exits.
- Each person should know the predetermined assembly point where everyone can be accounted for (e.g., across the street or at a neighbor's house). Once everyone is out of the building, call the fire department.
- A good plan emphasizes quick escape. Do not investigate or attempt to fight the fire, and do not gather belongings as this can waste valuable time. Once outside, do not re-enter the house. Wait for the fire department.
- Write the fire escape plan down and rehearse it frequently so that should an emergency arise, everyone will know what to do. Revise the plan as conditions change, such as the number of people in the home, or if there are changes to the building's construction.
- Make sure your fire warning system is operational by conducting weekly tests. If you are unsure about system operation, contact your installer.

We recommend that you contact your local fire department and request further information on fire safety and escape planning. If available, have your local fire prevention officer conduct an in-house fire safety inspection.



Figure 5

Carbon monoxide detectors

Carbon monoxide is colorless, odorless, tasteless, and very toxic, it also moves freely in the air. CO detectors can measure the concentration and sound a loud alarm before a potentially harmful level is reached. The human body is most vulnerable to the effects of CO gas during sleeping hours; therefore, CO detectors should be located in or as near as possible to sleeping areas of the home. For maximum protection, a CO alarm should be located outside primary sleeping areas or on each level of your home. Figure 5 indicates the suggested locations in the home.

Do NOT place the CO alarm in the following areas:

- Where the temperature may drop below -10°C or exceed 40°C
- Near paint thinner fumes
- Within 5 feet (1.5m) of open flame appliances such as furnaces, stoves and fireplaces
- In exhaust streams from gas engines, vents, flues or chimneys
- Do not place in close proximity to an automobile exhaust pipe; this will damage the detector

PLEASE REFER TO THE CO DETECTOR INSTALLATION AND OPERATING INSTRUCTION SHEET FOR SAFETY INSTRUCTIONS AND EMERGENCY INFORMATION.

Regulatory Agency Statements

FCC COMPLIANCE STATEMENT

▲ CAUTION: Changes or modifications not expressly approved by Digital Security Controls could void your authority to use this equipment.

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

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

The user may find the following booklet prepared by the FCC useful: 'How to Identify and Resolve Radio/Television Interference Problems'. This booklet is available from the U.S. Government Printing Office, Washington D.C. 20402, Stock # 004-000-00345-4.

The keypads represented in this manual can be used with the following Control Units: HS3032, HS3128, and HS3248

IMPORTANT INFORMATION

This equipment complies with Part 68 of the FCC Rules and, if the product was approved July 23, 2001 or later, the requirements adopted by the ACTA. On the side of this equipment is a label that contains, among other information, a product identifier. If requested, this number must be provided to the Telephone Company.

HS3032 Product Identifier US:F53AL01AHS3256

HS3128 Product Identifier US:F53AL01AHS3256

HS3248 Product Identifier US:F53AL01AHS3256

USOC Jack: RJ-31X

Telephone Connection Requirements

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

Ringer Equivalence Number (REN)

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local Telephone Company. For products approved after July 23, 2001, the REN for this product is

part of the product identifier that has the format US: AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Incidence of Harm

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. But 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 it is necessary.

Changes in Telephone Company Equipment or Facilities

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 necessary modifications to maintain uninterrupted service.

Equipment Maintenance Facility

If trouble is experienced with this equipment for repair or warranty information, contact the facility indicated below. If the equipment is causing harm to the telephone network, the Telephone Company may request that you disconnect the equipment until the problem is solved. This equipment is of a type that is not intended to be repaired by the end user. Tyco Atlanta Distribution Center, 2600 Westpoint Dr., Lithia Springs, GA 30122

Additional Information

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information. Alarm dialing equipment must be able to seize the telephone line and place a call in an emergency situation. It must be able to do this even if other equipment (telephone, answering system, computer modem, etc.) already has the telephone line in use. To do so, alarm dialing equipment must be connected to a properly installed RJ-31X jack that is electrically in series with and ahead of all other equipment attached to the same telephone line. Proper installation is depicted in the figure below. If you have any questions concerning these instructions, you should consult your telephone company or a qualified installer about installing the RJ-31X jack and alarm dialing equipment for you.

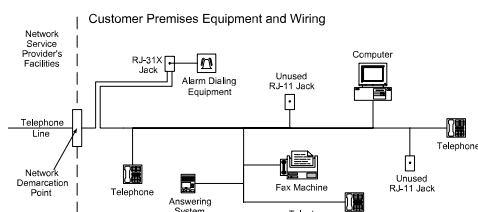


Figure 6

INNOVATION, SCIENCE & ECONOMIC DEVELOPMENT CANADA (ISED CANADA)

Notice: The models HS3032, HS3128, and HS3248 meet the applicable ISED Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, ISED, before the registration number signifies that registration was performed based on a

Declaration of Conformity indicating that ISED Canada technical specifications were met. It does not imply that ISED Canada approved the equipment.

The Ringer Equivalence Number (REN) for this terminal equipment is 0.1. The REN assigned to each terminal equipment 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 devices does not exceed 5.

HS3032 Registration number IC:160A-HS3256

HS3128 Registration number IC:160A-HS3256

HS3248 Registration number IC:160A-HS3256

FCC AND ISED CANADA FOR WIRELESS KEYPADS

▲ WARNING: To comply with FCC and ISED Canada RF exposure compliance requirements, the HS2LCDRFPRO9 or HS2LCDWFPRO9, and HS2LCDWVPRO9 keypads should be located at a distance of at least 20 cm from all persons during normal operation. The antennas used for this product must not be co-located or operated in conjunction with any other antenna or transmitter. This device complies with FCC Rules Part 15 and with ISED Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference that may be received or that may cause undesired operation.

IC:160A – HS2KRFP9

Models: HS2LCDRFPRO9, HS2LCDWFPRO9, HS2LCDWVPRO9 (operating in 912-919MHz band) are compliant with applicable FCC Part 15.247 and IC RSS-210 rules.

The term “IC” before the radio certification number only signifies that ISED Canada technical specifications were met.

Avertissement: Pour répondre aux exigences de conformité de la FCC et ISDE Canada sur les limites d'exposition aux radiofréquences (RF), les clavier HS2LCDRFPRO9 ou HS2LCDWFPRO9, HS2LCDWVPRO9 doivent être installés à une distance minimale de 20 cm de toute personne lors de leur fonctionnement usuel. Ces derniers ne doivent pas être situés au même endroit, ni être en fonction avec une autre antenne ou un autre transmetteur. Le présent appareil est conforme aux CNR ISDE Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

EN Compliance

This product meets the requirements of Class II, Grade 3 equipment as per EN 50131-1:2006 + A1:2009 +A2:2017 Standard. This product is suitable for use in systems with the following notification options:

- A (use of two remotely powered warning devices and single path SP3 internal dialer or Ethernet path or plug-in cellular module required),
- B (self powered warning device (wireless siren) and single path SP3 internal dialer or Ethernet path or plug-in cellular module required),
- C (dual path DP2 internal dialer and alternate Ethernet or plug-in cellular communicator required)
- D (single path SP4 internal Ethernet path or plug-in cellular communicator with encryption enabled required)
- E (dual path DP3 internal Ethernet path and plug-in cellular communicator required)

The Model HS3032, HS3128, and HS3248 Control panels have been certified by Telefication according to EN50131-1:2006 + A1:2009 +A2:2017, EN50131-3:2009 Type B, EN50131-6:2017 Type A, EN50131-10:2014 and EN50136-2:2013 for Grade 3, Class II, ATS Configurations SP3 (phone line path only), SP4 (Ethernet or cellular path only), DP2 (dual path with phone line primary path and Ethernet or Cellular secondary path) and DP3 (dual path with Ethernet or Cell primary path and Cellular or Ethernet as secondary path).

EUROPEAN CE COMPLIANCE STATEMENT

This product is in conformity with the Electromagnetic Compatibility Directive 2014/30/EU, the Low Voltage Directive 2014/35/EU, and the ROHS3 Directive (EU)2015/863.

Simplified EU Declaration of Conformity

Hereby, Tyco Safety Products Canada Ltd declares that the radio equipment type is in compliance with Directive 2014/53/EU. The full text of the EU declarations of conformity for the models mentioned below are available at the following internet addresses:

HS2LCDPRO: <http://dsc.com/pdf/1903004>

HS2TCHPRO(BLK): <http://dsc.com/pdf/1903007>

HS2LCDRFPRO4: <http://dsc.com/pdf/1903008>

HS2LCDRFPRO8: <http://dsc.com/pdf/1903005>

HS2LCDWF(V)PRO8: <http://dsc.com/pdf/1903009>

HS2LCDWF(V)PRO4: <http://dsc.com/pdf/1903007>

Frequency Band / Maximum Power

433.22MHz – 434.62MHz/10mW

868.0MHz – 868.6MHz/10mW

868.7MHz – 869.2MHz/10mW

119MHz – 135MHz - 66 db μ A/m @10m

European single point of contact: Tyco Safety Products, Voltaweg 20, 6101 XK Echt, Netherlands

UK Compliance Statement

In the UK this product is suitable for use in systems installed to conform to PD 6662:2017 at Grade 3 and environmental class II with the following notification options: A, B, C, D, E.

Where HS3032, HS3128, and HS3248 are used with a single path signaling method (such as the Integrated Digital Dialer), please note the following limitation:

Important

Your attention is drawn to the fact that failure or compromise of single path signaling cannot be passed to the police. While the failure persists, subsequent alarms cannot be notified to the alarm receiving centre and passed to the police.

Setting Methods

The HS3032, HS3128, and HS3248 are capable of supporting the completion of the full setting procedure by the following methods:

a) push button switch, mounted outside the supervised premises; or b) protective switch (i.e., door contact) fitted to the final exit door of the alarmed premises or area. The setting procedure is a two-stage process of initiating the setting procedure within the supervised premises (e.g., using Mini Prox Tag (MPT) or user code) followed by completion of setting by one of the two methods mentioned above. Please check with the Installer which method has been enabled for your system.

Unsetting Methods

The HS3032, HS3128, and HS3248 are capable of supporting the following unsetting methods in accordance with BS8243:

6.4.2 Prevention of entry to the supervised premises before the alarm system is unset. Unsetting using remote key before entering the supervised premises causes or permits the initial entry door to be unlocked.

6.4.5 Completion of unsetting using a digital key (e.g., MPT or PG8929, PG8939, PG8949) either before entering the protected premises (use PG8929, PG8939, PG8949) or after entering the protected premises (use MPT). The entry delay is activated if the initial entry door is opened before the HS3032, HS3128, HS3248 has been unset. During the entry time, it is possible to unset the alarm system using a digital key only. Complete unsetting before programmed entry delay expires.

Important

If using a remote device to remotely set/unset your intruder alarm system, your attention is drawn to the fact that whenever a premises is unattended but its intruder alarm system(s) is (are) not fully set, any related insurance cover might be inoperative. For advice on this matter, it is recommended that you consult your insurer(s)."

New Zealand Telecom Network Warnings

The following is a list of warnings that are applicable when the HS3248, HS3128, HS3032 equipment is connected to the New Zealand telecom network.

When a Telepermit is granted for any item of terminal equipment, it indicates only that telecom has accepted that the item complies with minimum conditions for connection to its network. It does not indicate endorsement of the product by telecom, nor does it provide any sort of warranty. It does not indicate that equipment will work correctly with another item of equipment of a different make or model that has a Telepermit. A Telepermit does not indicate that any product is compatible with all of telecom's network services.

Reverse numbering -decadic signalling

Do not use decadic signaling. DTMF dialing is available and it should always be used.

Line grabbing equipment

This equipment is set up to complete test calls at pre-determined times. Test calls will interrupt any other calls that are set up on the line at the same time.

① **Note:** Discuss timing sets with the installer.

The timing set for test calls from this equipment may be subject to 'drift'. If this proves to be inconvenient and calls are interrupted, discuss this with the equipment installer. The matter should NOT be reported as a fault to telecom Faults Service.

DC line feed to other devices

During dialing, this device unit does not provide DC voltage to the series port connection, this may cause loss of memory functions for the terminal devices (local telephone) connected to T-1 and R-1.

General operation -ringer sensitivity and loading

This device only responds to Distinctive Alert cadences DA1 and DA2. In the event of any problem with this device, disconnect it. Connect a CPE item connected to one of the device's terminal ports directly in its place.

➤ **Important:** Arrange for the product to be repaired. Should the matter be reported to telecom as a wiring fault, and the fault is proven to be due to this product, a call-out charge will be incurred.

EULA

IMPORTANT - READ CAREFULLY: DSC Software purchased with or without Products and Components is copyrighted and is purchased under the following license terms:

This End-User License Agreement (“EULA”) is a legal agreement between You (the company, individual or entity who acquired the Software and any related Hardware) and Digital Security Controls, a division of Tyco Safety Products Canada Ltd. (“DSC”), the manufacturer of the integrated security systems and the developer of the software and any related products or components (“HARDWARE”) which You acquired.

If the DSC software product (“SOFTWARE PRODUCT” or “SOFTWARE”) is intended to be accompanied by HARDWARE, and is NOT accompanied by new HARDWARE, You may not use, copy or install the SOFTWARE PRODUCT. The SOFTWARE PRODUCT includes computer software, and may include associated media, printed materials, and “online” or electronic documentation.

Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to You under the terms of that license agreement.

By installing, copying, downloading, storing, accessing or otherwise using the SOFTWARE PRODUCT, You agree unconditionally to be bound by the terms of this EULA, even if this EULA is deemed to be a modification of any previous arrangement or contract. If You do not agree to the terms of this EULA, DSC is unwilling to license the SOFTWARE PRODUCT to You, and You have no right to use it.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE This EULA grants You the following rights:

(a) Software Installation and Use - For each license You acquire, You may have only one copy of the SOFTWARE PRODUCT installed.

(b) Storage/Network Use - The SOFTWARE PRODUCT may not be installed, accessed, displayed, run, shared or used concurrently on or from different computers, including a workstation, terminal or other digital electronic device (“Device”). In other words, if You have several workstations, You will have to acquire a license for each workstation where the SOFTWARE will be used.

(c) Backup Copy - You may make back-up copies of the SOFTWARE PRODUCT, but You may only have one copy per license installed at any given time. You may use the back-up copy solely for archival purposes. Except as expressly provided in this EULA, You may not otherwise make copies of the SOFTWARE PRODUCT, including the printed materials accompanying the SOFTWARE.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

(a) Limitations on Reverse Engineering, Decompilation and Disassembly - You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to the Software, without the written permission of an officer of DSC. You may not remove any proprietary notices, marks or labels from the Software Product. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA.

(b) Separation of Components - The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one HARDWARE unit.

(c) Single INTEGRATED PRODUCT - If You acquired this SOFTWARE with HARDWARE, then the SOFTWARE PRODUCT is licensed with the HARDWARE as a single integrated product. In this case, the SOFTWARE PRODUCT may only be used with the HARDWARE as set forth in this EULA.

(d) Rental - You may not rent, lease or lend the SOFTWARE PRODUCT. You may not make it available to others or post it on a server or web site.

(e) Software Product Transfer - You may transfer all of Your rights under this EULA only as part of a permanent sale or transfer of the HARDWARE, provided You retain no copies, You transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades and this EULA), and provided the recipient agrees to the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade, any transfer must also include all prior versions of the SOFTWARE PRODUCT.

(f) Termination - Without prejudice to any other rights, DSC may terminate this EULA if You fail to comply with the terms and conditions of this EULA. In such event, You must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

(g) Trademarks - This EULA does not grant You any rights in connection with any trademarks or service marks of DSC or its suppliers.

3. COPYRIGHT - All title and intellectual property rights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, and text incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by DSC or its suppliers. You may not copy the printed materials accompanying the SOFTWARE PRODUCT. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE PRODUCT are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants You no rights to use such content. All rights not expressly granted under this EULA are reserved by DSC and its suppliers.

4. EXPORT RESTRICTIONS - You agree that You will not export or re-export the SOFTWARE PRODUCT to any country, person, or entity subject to Canadian export restrictions.

5. CHOICE OF LAW - This Software License Agreement is governed by the laws of the Province of Ontario, Canada.

6. ARBITRATION - All disputes arising in connection with this Agreement shall be determined by final and binding arbitration in accordance with the Arbitration Act, and the parties agree to be bound by the arbitrator's decision. The place of arbitration shall be Toronto, Canada, and the language of the arbitration shall be English.

7. LIMITED WARRANTY

(a) NO WARRANTY - DSC PROVIDES THE SOFTWARE "AS IS" WITHOUT WARRANTY. DSC DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

(b) CHANGES IN OPERATING ENVIRONMENT - DSC shall not be responsible for problems caused by changes in the operating characteristics of the HARDWARE, or for problems in the interaction of the SOFTWARE PRODUCT with non-DSC-SOFTWARE or HARDWARE PRODUCTS.

(c) LIMITATION OF LIABILITY; WARRANTY REFLECTS ALLOCATION OF RISK - IN ANY EVENT, IF ANY STATUTE IMPLIES WARRANTIES OR CONDITIONS NOT STATED IN THIS LICENSE AGREEMENT, DSC'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS LICENSE AGREEMENT SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU TO LICENSE THE SOFTWARE PRODUCT AND FIVE CANADIAN DOLLARS (CAD\$5.00). BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

(d) DISCLAIMER OF WARRANTIES - THIS WARRANTY CONTAINS THE ENTIRE WARRANTY AND SHALL BE IN LIEU OF ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED (INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE) AND OF ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF DSC. DSC MAKES NO OTHER WARRANTIES. DSC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT

ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE PRODUCT.

(e) EXCLUSIVE REMEDY AND LIMITATION OF WARRANTY - UNDER NO CIRCUMSTANCES SHALL DSC BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES BASED UPON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER LEGAL THEORY. SUCH DAMAGES INCLUDE, BUT ARE NOT LIMITED TO, LOSS OF PROFITS, LOSS OF THE SOFTWARE PRODUCT OR ANY ASSOCIATED EQUIPMENT, COST OF CAPITAL, COST OF SUBSTITUTE OR REPLACEMENT EQUIPMENT, FACILITIES OR SERVICES, DOWN TIME, PURCHASERS TIME, THE CLAIMS OF THIRD PARTIES, INCLUDING CUSTOMERS, AND INJURY TO PROPERTY.

⚠ WARNING: DSC recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this SOFTWARE PRODUCT to fail to perform as expected.

Always ensure you obtain the latest version of the User Guide. Updated versions of this User Guide are available by contacting your distributor.

Trademark

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

© 2021 Johnson Controls. All rights reserved. JOHNSON CONTROLS, TYCO and DSC are trademarks and/or registered trademarks. Unauthorized use is strictly prohibited.

Toronto, Canada · www.dsc.com

Tech support: 1-800-3630 (Canada and U.S), or 1-905-760-3036 (International)
