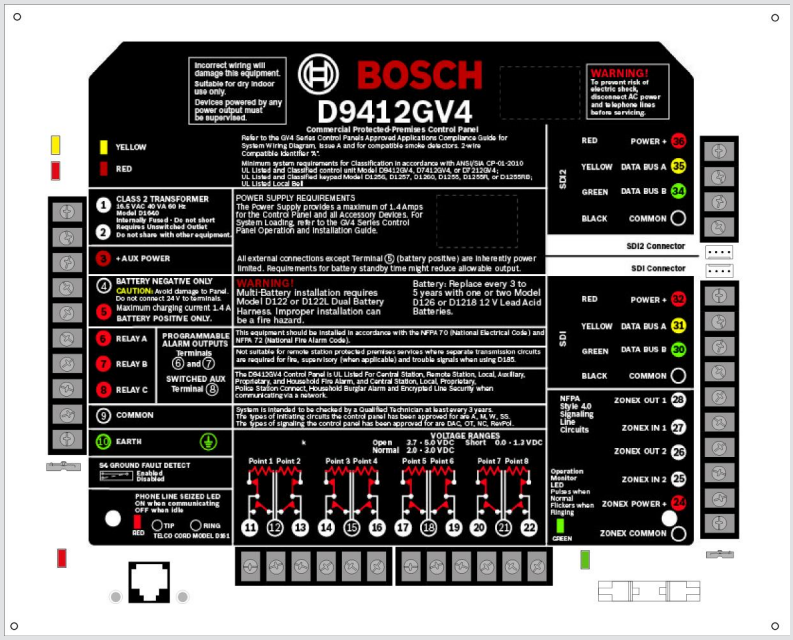


Control Panels

D9412GV4/D7412GV4 v2.03.018

BOSCH

en Release Notes

Table of contents

1 Introduction

These *Release Notes* are for control panel **firmware v2.03.018**

1.1 Requirements

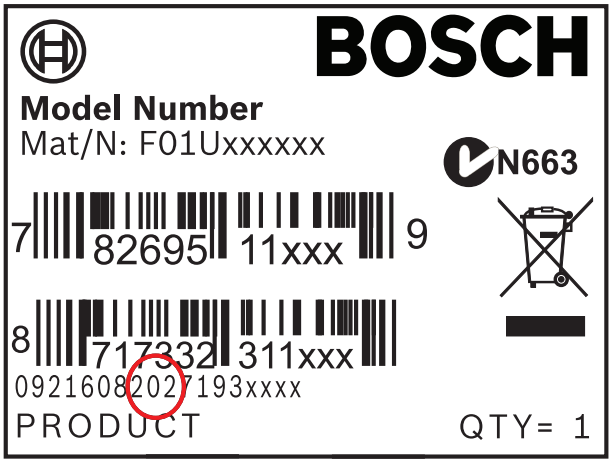
Firmware v2.03 requires Remote Programming Software (RPS) version 5.19 or higher to fully program the control panel.

1.2 About documentation

Copyright

Use the serial number located on the product label and refer to the Bosch Security Systems, Inc. website at http://www.boschsecurity.com/datecodes/.

The following image shows an example of a product label and highlights where to find the manufacturing date within the serial number.



Trademarks

All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly.

1.2.1 Related documentation

Description	Part Number
Control Panels (D9412GV4/D7412GV4 v2.02) Program Entry Guide	F01U265459
D9412GV4/D7412GV4/D7212GV4 Program Record Sheet	F01U214958
UL Certificated Bank Safe and Vault Applications Technogram	73-07302-000
D9412GV4/D7412GV4 v2.00 Control Panels Quick Reference Guide	F01U265463
Control Panels (D9412GV4/D7412GV4 v2.02) Installation and System Reference Guide	F01U265457
Control Panels (D9412GV4/D7412GV4 v2.00 and higher) SIA Quick Reference Guide	F01U265466

Control Panels (D9412GV4/D7412GV4 v2.02) UL Installation Guide	F01U291483
Basic Keypad (B915) Installation Guide	F01U297873
Two-line Alphanumeric Keypad (B920) Installation Guide	F01U265450
Two-line Capacitive Keypad (B921C/B921CW) Installation Guide	F01U285416
ATM Style Alphanumeric Keypad (B930) Installation Guide	F01U265451
Touch Screen Keypad (B942) Installation Guide	F01U285416
Control Panels (D9412GV4/D7412GV4 v2.02) Owner's Manual	F01U287176
Octo-input Module (B208) Installation and Operation Guide	F01U265456
Octo-output Module (B308) Installation and Operation Guide	F01U265458
RADION receiver SD (B810) Reference Guide	F01U261839
SDI2 Inovonics Interface Module (B820) Installation Guide	F01U265460
Conettix Plug-in Communicator Interface (B450) Installation and Operation Guide	F01U300740
Conettix Ethernet Communication Module (B420) Installation and Operation Guide	F01U215236
Conettix Ethernet Communication Module (B426) Installation and Operation Guide	F01U266226
Auxiliary Power Supply Module (B520) Installation and Operation Guide	F01U265445
D8128D Installation Guide	F01U070537
D8125MUX Operation and Installation Guide	F01U034973
ISW-D8125CW-V2 Installation and Operation Guide	F01U161691
D9210C Installation and Operation Guide	F01U215232

1.3 Important pre-upgrade information

Please read through this important information prior to beginning your control panel upgrade from GV4 v1.xx to GV4 v2.xx.
Following control panel upgrade, SDI2 keypads have full functionality (SDI keypads operate with some limitations).

Notice!
Upgrading the system sets the control panel to factory default configuration. Prior to the upgrade, disconnect the on-board relays, relay modules, and all keypads until the system is properly re-configured.

Notice!

Before upgrading a v1.xx GV4 control panel to a v2.xx, please understand: Full functionality is available only with the B Series keypads (B915/B920/B921C/B930/B942), SDI keypads only have limited functionality. Once you have upgraded an RPS account, you cannot down-grade the account. If you are down-grading the control panel, you are required to recreate the entire account in RPS.

RPS accounts upgrade

Upgrade an existing G Series control panel account to a GV4 v2.xx account using the latest version of RPS. Refer to the *RPS HELP* for the specific control panel for additional information on control panel account conversion. In the *RPS HELP* file, select:
Panel Specific Information→Communicating with 9000 Series Panels→Upgrading a Panel Type.

Hardware upgrade

– The GV4 control panel's terminal blocks, SDI quick-connect terminal, and accessory connector are all fully compatible with all G series and GV2 series control panel peripherals.

1.3.1 GV4 firmware version updates

Firmware version 2.xx updates are available via a network connection or Blue ROM update key (GV4-ROM-KEY), and are also available via a firmware download at: us.boschsecurity.com. Firmware version 2.xx updates may be performed via USB or serial connection using the DX4010V2.

Perform the procedure below to access firmware updates from the website:

Downloading firmware updates:

1. Go to the Bosch website (us.boschsecurity.com).
2. In the Search text box on the right side of the page, enter the CTN (product name) for the product for which you wish to download the firmware.
3. Press [ENTER].
4. In the Search Results area, click the desired product's Product Page button. The product page opens with the Details tab selected.
5. Click on the Software Downloads tab, and then click the desired language listed to the right of the desired firmware.

Call Bosch Security Systems, Inc., Technical Support (1-800-289-0096) if you need additional assistance.

1.3.2 How to convert GV4 v1.xx to GV4 v2.xx

Please reference the following procedure to convert a GV4 v1.xx account to a GV4 v2.xx account. Due to the fundamental differences in the firmware between the GV4 v1.xx and GV4 v2.xx, it is important to follow this process. Note that after the update of the firmware from v1.xx to v2.xx, the configuration values will be set to default.

1. Use the latest version of RPS.
2. To import the new firmware into RPS, follow *Steps 3* through 5.
3. From the Main menu, select **Config** > **System**. Select the **GV4 Firmware Files** tab, and then click **Import.**
4. Click **Select Firmware File** ellipsis (browse) button and then browse to and select the firmware file to upload.
5. Click **Open** and then **Next**. When the import finishes complete click **Finish/**
6. To create a backup copy of the control panel account, follow *Steps 7* through *9***.**

7. From the **Panel List** window, click **New.**
8. To create a new panel from one currently in the panel list, from the **New Panel** window, click the **Existing** tab. Select the control panel account from the list of existing panels, and click **OK.**
9. Fill in the appropriate parameters to create the GV4 Version 2.xx control panel account and click **OK.**
10. You can perform upgrades using RPS via a network connection, or a USB or serial connection using the DX4010V2.
11. Open the GV4 v1.xx control panel account and connect to the GV4 v2.xx control panel.
12. Click the **Firmware Update Wizard** icon. The **Firmware Update Wizard** opens.
13. Click **Next** and select the correct firmware file and click **Next.**
14. Select the **Acknowledge to Continue** check box and click **Next** to begin the upgrade. When the update finishes, the **Disconnecting from the Control Panel** message appears.
15. Click **Close**. The control panel reboots.
16. To update the RPS control panel account, follow *Steps 17* through *20*.
17. Close the control panel account by clicking the **Close** button. Select the upgraded control panel which is highlighted in the Panel List.
18. Right-click on the highlighted, updated control panel and select **View.**
19. In the control panel **Data View** window, click **Edit** and then select the drop-down arrow beside the **Panel Type** box.
20. From the **Panel Type** drop down list, select the correct control panel type with [**V2.00 or greater**] (i.e. D9412GV4 v2.00 or greater) and then click **OK.**
21. To reconnect to the control panel and send the update to the control panel, follow *Steps 22* through *23*.
22. Open the **Version 2.xx** control panel account and connect to the control panel. The **Panel Sync** dialog box appears.
23. Select **Send Only Updated RPS Data to Panel**. Note: Do not select **Receive Panel Data**, and click **OK.**
24. The firmware update completes and you can exit RPS.
25. Test the control panel for operation.

Notice!

After system installation and any control panel programming, perform a complete system test (a UL864 requirement). A complete system test includes testing the control panel, all devices, and communication destinations for proper operation.

2 Version 2.03.018 firmware

Corrections

Known issues

2.1 Corrections

This section examines the corrections made in this firmware version.

2.1.1 Incorrect report delivery confirmation

The following is resolved in this firmware version: In rare cases when attempting to send a network report to the central station, the control panel might misinterpret a receiver supervision poll response as a report transmission response. Although all local devices (e.g. keypad displays, sounders, and bells) provide proper event indications, the central station receiver might not receive the report. This scenario erroneously indicates that the central station receiver properly received the report. This only affects customers using Ethernet or cellular as a primary or backup device with the Receiver Supervision Time set to a value other than “No Polling”.

2.1.2 B942/B942W keypad inactivity

The following is resolved in this firmware version: A B942/B942W Touch screen Keypad might show flashing text or might reset. As part of the reset process, the keypad stops responding to the control panel for approximately 15 seconds, and then resumes normal operation. The control panel creates a missing keypad event, and if points are assigned to that keypad, the control panel creates missing point events, followed by their restorals.

2.1.3 Off-normal Test Reports sent for faulted controlled points

The following is resolved in this firmware version: At the time of a manually or scheduled Test Report, the control panel sends an Off-Normal Test Report if any controlled point is faulted.

2.2 Known issues

This section examines the known issues of this firmware version.

2.2.1 Wireless

– Replacing a wireless point device that has a low battery condition with a different device does not restore the point; replace the batteries of the device with the low battery condition to generate a restoral event.

- Using a keypad to change the RF ID of an RFUN transmitter, when the RFUN has only one Input Function enabled, generates a false trouble.
- When an RFUN universal transmitter is tampered, the keypad indicates that the point is Open. To determine whether the point is open or tampered without examining the device, enter the keypad's Installer menu, and then view the Diagnostics for RF Points within the Wireless menu.

2.2.2 Direct connect (AutoIP) RPS sessions

- If Ethernet communication items are changed during an RPS direct-connect (AutoIP) session, subsequent direct-connect sessions require that the Ethernet cable be removed and then reconnected.

2.2.3 Sensor Reset Command (COMMAND 47)

- On the D1260 and D1260B Keypads, when the Sensor Reset command (COMMAND 47) is executed, Call for Service appears erroneously on the display for a brief time. This effect also occurs when the control panel reboots.

2.2.4 ANSI SIA CP-01

Change the Service Passcode (User ID 0) factory default value when the ANSI SIA CP-01 required Passcode Length parameter is 4 or greater.

2.2.5 ITS-DX4020-G

- When using an ITS-DX4020-G as a GSM phone device, the central station phone number must have a dial pause (C) option as the first digit.

2.2.6 Single RPS connection

- Only one connection to RPS can be made. RPS will notify you if you are already in a connection.

2.2.7 Area Assigned

When configuring a custom area scope for a keypad, always include the Area Assigned. Failure to do so results in inconsistent operation.

2.2.8 Conversion issues (GV4 v1.xx to GV4 v2.xx)

- Custom functions are done differently in GV4 v2.xx. Custom functions from GV4 v1.00 cannot be converted to new custom function in the GV4 v2.xx account on an account upgrade.
- Fire point has been removed as a Point Index parameter; it is now Point Type.
- You will need to contact your central station to re-synchronize the Anti-Replay/Anti-Substitution feature.
- The control panels event log will be reset.
- Some point types that are no longer supported, D279 (O/C Non-Priority), D279 (O/C Non-Priority), and Easikey. When these point types are detected in a GV4 v1.00 they will be converted to Point Type = 24-Hour.

2.2.9 False communication troubles

When reporting over Ethernet or cellular and configured with a primary and backup path to the same receiver, or with two route groups going to the same receiver, the system may fail to send events without waiting configured ACK-wait time or using retries. This generated COMM. troubles with immediate restorals. This issue has been resolved in v2.02.

2.2.10 Reporting Delay for Single Tower

This parameter allows the control panel to indicate if there is only one tower available for communication if the event has been present for the duration specified. Leave this parameter at the default setting (0 Disabled) unless otherwise instructed by a Bosch Security Systems, Inc. representative.

2.2.11 GV4 known issues

– GV4 v2.03. RPS diagnostics for the B450 Conettix Plug-in Communicator Interface are only available when the module is set to address 1. When the module is set to address 2, the B450 Conettix Plug-in Communicator Interface is fully functional, however, RPS diagnostics are not available.

2.2.12 Two-man rule duress token failure

Bosch highly recommends against using access credentials for duress if the system is programmed for two man rule as this could possibly fail to report duress events.

3 Firmware revision history

This section examines the notable features of previous revisions of this firmware.

3.1 Version 2.03.010 firmware revision history

Notable features

3.1.1 B915 Basic keypad support

The B915 Basic Keypad is an SDI2 bus compatible device. It offers the same commands and menu structure as the other B Series intrusion keypads.

3.1.2 B942/B942W Touch Screen Keypad support

The B942/B942W is an SDI2 bus compatible device. Each keypad has a credential reader, a presence sensor, a graphical interface for controlling the system, touch screen keys for data or command entry, a backlit display that shows system messages for all areas, and a user-adjustable sounder that emits warning tones. The keypad supports four inputs and one output.

3.1.3 B942/B942W keypad output support

The control panel supports the B942/B942W output connection, which provides for cost effective expansion.

3.1.4 Keypad proximity reader support

The control panel supports the proximity reader on compatible keypads, such as the B942/B942W. The reader allows for an optional credential (card or token) to turn on or off the security system without pressing any keys. The user simply swipes a card or token in front of the keypad’s integrated reader.

3.1.5 B450 module support

The B450 is a four-wired SDI2 bus device that supports two-way IP communication over commercial cellular networks using a plug-in communicator. The module allows remote location installation of plug-in cellular communicators, and allows a plug-in cellular communicator installation through the SDI2 when a B430 Plug-in Telephone Communicator is connected to the control panel.

Supported cellular plug-in modules include:

– B440 Conettix Plug-in Communicator, Cellular (3G)
– B441 Conettix Plug-in CDMA Cellular Communicator
– B442 Conettix Plug-in GPRS Cellular Communicator (intended for Europe, Latin America, Middle East, Australia, and China)
– B443 Conettix Plug-in HSPA+ Cellular Communicator (intended for Canada, Europe, and Middle East)

3.1.6 B442 and B443 module support

The control panel supports the new B442 Plug-in GPRS Cellular Communicator and B443 Plug-in HSPA+ Cellular Communicator through the use of the B450 Conettix Plug-in Communicator Interface. The B442 provides IP communication over a GSM (GPRS) cellular network. The B443 enables IP communication over a GSM/GPRS/EDGE/UMTS/HSPA cellular network.
The B442 is for use in Latin America, Europe, Middle East, Australia, and China. The B443 is for use in Canada, Europe, and Middle East regions.

3.1.7 Passcode Enter function

For SDI2 keypads, the control panel provides additional passcode enter functions on supported v2.03 systems to increase user convenience. These are especially useful when used with the new B942/B942W Touch Screen keypad.
These passcode enter functions are Login Only and Login/Disarm.

Login Only

When a user logs in, the control panel toggles to the configured user language, and silences any bells.

Login/Disarm

When using this feature, the control panel toggles to the configured user language, deactivates any active bells, and disarms any armed areas within the scope of the keypad in reference to the authority level of the designated user.

3.1.8 Bus module diagnostics

The control panel supports bus module diagnostics for cellular devices connected through the B450. Diagnostic information shows within the module diagnostics, and can show on the keypad and in RPS.

3.2 Version 2.02 firmware revision history

Notable features

3.2.1 Monitor Delay

Use this parameter to configure the length of time (MM:SS) a control panel waits after a disarmed point has been faulted before logging and/or reporting the event to the central station receiver. The control panel logs and reports a Burg Supervisory report to the central station receiver if the point remains faulted during the entire period of time configured in this parameter. If the point is restored during this time, the control panel does not send a report. There is no audible or visual annunciation of the report sent to the central station receiver.
To enable the reporting portion of this feature, additionally set the Disarmed Point Response to “Blank”.

Example of use for this feature would be to notify the central station if a freezer or overhead door has been left open for an extended amount of time.

3.2.2 Delay Response

For special applications, this configurable timer requires an extended fault duration before an off-normal condition is recognized. This feature is useful to allow a site to create an alarm or local warning when a point remains faulted too long (or requires a longer point response time), such as an employee door, or overhead door. There is a separate delay configuration for armed and disarmed states. Most point responses are delayed, including alarm detection, watch tone, output followers, buzz on fault.
24-Hour points always use the **Delay Response, Armed** feature even if the area is disarmed.

Delay response – disarmed
This feature sets the length of time (MM:SS) the control panel waits after a point faults before annunciating or reporting the fault. You can set this parameter from 5 seconds to one hr. This parameter only applies to the following point types when disarmed:
– Part On
– Interior
– Interior Follower

Default: 00:00
Selections: 00:05 thru 60:00
00:00 = Disabled

Delay response – armed
This parameter sets the length of time (MM:SS) the control panel waits after an armed point faults before annunciating or reporting the fault. This parameter only applies to the following point types when armed:
– 24-Hour
– Part On
– Interior
– Interior Follower

Default: 00:00
Selections: 00:05 thru 60:00
00:00 = Disabled

3.2.3 Area Re-Arm

Area Re-Arm allows high security areas such as vaults and ATM machines to automatically rearm after a configured amount of time (HH:MM). This prevents scenarios where the user disarms, finishes his task, but forgets to rearm. There is an optional “Close now” warning 10 min before it arms, and the area annunciates exit delay warning if exit delay is configured. When enabled, the control panel automatically starts a timer to rearm an area when that area has been disarmed.
The default timer is disabled with a value set of 00:00, but has a range of 23:59 (23 hr and 59 min) when enabled.

Notice!
The designated area rearms automatically at midnight regardless of how much time has elapsed.
Area rearms to All On regardless of the previous arm state.

3.2.4 Enhanced keyfob operation

The control panel includes an option to have greater flexibility regarding user authority related to the arming and disarming programming of the keyfob. The new parameters are;

– Keyfob Arm
– Keyfob Disarm

Keyfob authority allows you to configure a keyfob for either arming, disarming, or both. You can configure one user's keyfob to arm the system only, while another user's keyfob to disarm the system.

3.2.5 Legacy commands

The control panel now supports the following commands.

Command	Function
[CMD] 0	Bypass
[CMD] 0 0	Unbypass
[CMD] 1	All on (with delay)
[CMD] 1 1	All On, Instant
[CMD] 2	Part On, Instant
[CMD] 3	Part On (with delay)
[CMD] 4 0	See Alarms
[CMD] 4 7	Reset Sensors
[CMD] 5 0	Go to Area
[CMD] 5 1	Extend Close
[CMD] 5 3	Delete User
[CMD] 5 5	Change Passcode
[CMD] 5 6	Add User
[CMD] 5 9	Show Revision
[CMD] 6	Watch Mode
[CMD] 8	Open Main menu

The firmware version for which the legacy commands became available:

Firmware version	Legacy command
v2.03	[CMD] 8
v2.02	[CMD] 5 0, [CMD] 5 3, [CMD] 5 5, [CMD] 5 6, [CMD] 5 9
v2.00	[CMD] 0, [CMD] 0 0, [CMD] 1, [CMD] 1 1, [CMD] 2, [CMD] 3, [CMD] 4 0, [CMD] 4 7, [CMD] 6

Notice!
[CMD] 4 0 and [CMD] 8 are supported by SDI2 keypads only. [CMD] 5 6 on SDI keypads only adds the user and passcode; it does not support configuring user name, authority level, keyfob, and tokens and cards.

3.2.6 Remote module firmware updates

– The control panel includes the support of remote module firmware updating using the RPS Firmware Update Wizard – without visiting each individual module – via:
– Local – Ethernet or USB
– Remote – Ethernet or Cellular

The control panel includes a programmable option for local keypad authorization. When the local authorization option is enabled via RPS, only a user with the Firmware Update Authority enabled can authorize the update.

Preconditions
The control panel must be running normally: AC power present; the battery at full charge; and all areas disarmed. These three conditions must be met for firmware updates to initiate.

Notice!
When the firmware update completes and the control panel comes back on-line, the control panel generates a local restoral event for each module successfully updated. The events are local only.
You cannot update the firmware on a B426 or B450 module using the Firmware Update Wizard.

3.2.7 Monthly test reports

The control panel includes an option to enable monthly test reports. Monthly test reports run every 28 days without the need to program a SKED.

3.2.8 Keypad nightlight

Keypad nightlight is now supported on B921C, B920 and B930 keypads. There are two areas of illumination on the keypad. Those areas are:

– The display
– The keys on the keypad

The nightlight feature allows the keypad display and keys to be seen in a dark environment and has a “backlight” effect when the keypad is at an idle state (not in use and/or no active alarms).
Activation of this feature requires the keypad to have firmware version 1.01.007 or higher.
To enable the nighlight feature, perform the following:

At the keypad:
1. Press [MENU] to open the Main menu.
2. Use [NEXT] to go to the Press 5 for Settings Menu option, or simply press [5].
3. Use [NEXT] to go to the Press 4 for Keypad Config option, or simply press [4].
4. Use [NEXT] to go to the Press 4 for Nightlight option, or simply press [4].
5. Use [PREV] or [NEXT] to toggle between the Yes and No options.
6. Press [ENTER] while viewing the desired option to save the programming.
7. Press [ESC] to exit the menu.

In RPS

Program the nightlight feature using the latest version of RPS by selecting the SDI2 keypad option, and enable the feature.

3.2.9 Custom Function and SKED improvements

You can now toggle on-board outputs using SKEDS and Custom Functions. The output parameter for all SKED and Custom Functions include all on-board (1, 2, 3, (A, B, C)), off-board, and virtual outputs that are supported by the control panel.

3.2.10 Remote Security Control (RSC)

In addition to the iOS app, the control panel now supports an RSC app for Android.
Supported devices are:

- Android devices with Android version 2.3 (Gingerbread) or newer. Obtain the app through the Google Play Store.
- iPhone, iPod Touch, iPad with Apple iOS 4.5 or newer. Obtain the app through the iTunes App Store.

3.3 Version 2.00 firmware revision history

Notable features

3.3.1 New User interface

- New user interface. The new B930 and B920 keypads share a user interface with the B Series Control Panels.

3.3.2 Advanced custom functions

Simplified configuration

- Each function within a custom function is easily selectable and applied to areas using check boxes. Add custom (built-in) functions to keypad shortcuts.

Point initiated

- Custom functions can be initiated from a SKED, keypad, keyfob, or by faulting a point.

3.3.3 32 character text

The following 32 character texts are available on the B920/B930:

- User names
- Point names
- Area names

3.3.4 RADION wireless

- GV4 Series control panels at version 2.00 or higher now support the RADION family of wireless receivers, transmitters, and repeaters, just like B Series Control Panels.
- GV4 Series control panels only support one B810 RADION wireless module at a time, regardless of how many SDI2 buses are supported.

Keyfob initiated

- Add up to two custom functions to the RADION keyfob so that users can initiate custom functions with the touch of a button.

3.3.5 B920/B930 keypads

- GV4 Series control panels now support the B930 ATM Style Alphanumeric and B920 Two-line Alphanumeric keypads, just like B Series control panels.
- B920 features a bright, two line display with 8 function keys.
- B930 features a bright, five-line display with four ATM style softkeys on either side of the display.

3.3.6 Legacy keypads

- GV4 Series control panels continue to support legacy keypads such as the D1255, D1260, and D1265 with a limited command set.
- D1256RB remains fully functional and is required to meet UL864.

3.3.7 IPv6

- GV4 Series control panels now support the IPv6 communication protocol when using the B426 Ethernet Communication Module.

3.3.8 Gas alarm support

- GV4 Series control panels and B920/B930 Keypads support Gas alarm events.
- Gas alarm support includes the following conditions: Gas Alarm, Gas Trouble, and Gas Supervisory.
- Gas Alarm conditions are audibly represented at the keypads with a unique alarm tone (Temporal Code 4) different from fire and burglary tones. The control panel shall activate the gas alarm tone in the SDI2 keypads and the fire alarm tone in the SDI keypads.

3.3.9 Remote security control updates

- Supports Apple devices with iOS4.5 or greater.
- Allows users to arm/disarm areas, activate outputs and control doors to which they have assigned privileges.
- Full support of cellular connectivity at the panel.
- Updates are available via iTunes.

3.3.10 Reporting formats

- GV4 Series control panels now support Modem4 communication and contact ID reporting formats, just like B Series Control Panels.
- The use of Modem4 requires an update to the central station receiver for proper functionality and operation.
- Reporting events over the network, either by wired, or wireless, the reports are transmitted via Modem4 format.
- All events pertaining to SDI2 devices are supported with up to 4-digit device numbers.
- 10 digit Contact ID account numbers - entering an account number with more than 4 digits will turn on 10 digit account number reporting. This will require the central station receiver to be able to accept 10 digit Contact ID account numbers.

3.3.11 Shortcuts

- B920/B930 keypads include a configurable shortcut menu to quickly access common features that may be used the most.
- The GV4 Series control panel shortcuts include Cycle Door, Unlock Door, Lock Door, and Secure Door options.

3.3.12 Central Station requirements

If using Modem4

– The use of Modem4 communication format requires supporting central station receivers to be updated with the latest software. Modem4 will not work with receivers that have not been updated.

If using IPv6 protocol

– The use of the IPv6 communication protocol is optional. The new D6100IPv6 receiver supports IPv6 communication protocol.
– The new Conettix B426 Ethernet Communication Module supports IPv6 communication protocol. B426 is required in order to use IPv6.
– D6600 central station receivers must be updated with the latest software, and a new D6686 in order to communicate using IPv6 communication protocol.

4 Open source notifications

Bosch includes the open source software modules listed below in the firmware for this control panel. The inclusion of these modules does not limit the Bosch warranty.

Time routines

Copyright © 2002 Michael Ringgaard. All rights reserved.

This software [Time routines] is provided by the copyright holders and contributors "as is" and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the copyright owner or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

RSA data security

Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

The "RSA Data Security, Inc. MD5 Message-Digest Algorithm" is included in the control panel firmware.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

Bosch Security Systems, Inc.
130 Perinton Parkway
Fairport, NY 14450
USA
www.boschsecurity.com

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany