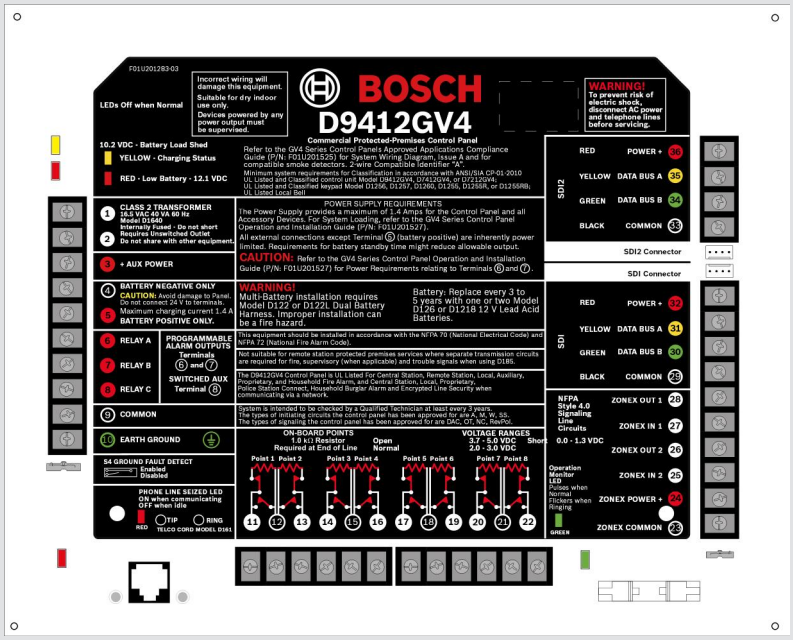

Control Panel

D9412GV4/D7412GV4/D7212GV4 Version 1.10

BOSCH

en Release Notes

Table of contents

1 Introduction

Requirements

Notice!
Use Remote Programming Software (RPS) version 5.14 and later with this software version. The D5200 Programmer is not supported by the GV4 Series control panel. The D5360 Direct Connect Module is not supported by the GV4 Series control panel. A limited programmers menu is available from the Service menu on the keypad.

1.1 About documentation

Copyright

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

1.2 Reading Bosch Security Systems, Inc. Product Date Codes

For Product Date Code information, refer to the Bosch Security Systems, Inc. web site at http://www.boschsecurity.com/datecodes.

2 Version 1.10

2.1 New

2.1.1 cUL Compliance

– GV4 is now cUL compliant for use in **Canada**. In order to meet Canadian requirements, the **Point/User Flag** parameter must be set to Yes. **Legacy Point/User Flag** functionality has been removed as of version 1.10.

2.2 Corrections

– The **Master Arm – No Exit** feature has been modified to process Interior Follower and Interior Delay points the same way (when faulted at the end of the exit delay time).
– Using the Modem IIIa2 communicator format**: Alarm**, **Recent Closing** and **Alarm, Exit Error** reports have been modified to send 3-digit point number reports.

2.3 Known Issues

2.3.1 Program Entry Guide Update

– *Section 3.10.5 Arming Features* of the *GV4 Series Program Entry Guide* (P/N: F01U218312) contains information for the A# Two Man Rule parameter that is incomplete. Use the following information in place of that found in the *Program Entry Guide*.

A# Two Man Rule

Default:	No
Selection:	Yes or No
Yes	Two different passcodes must be entered to disarm the area.
No	A single passcode can disarm the area.

The Two Man Rule feature is suitable for banks or other facilities that require a higher level of security to gain access to a vault or other protected area.
Use the parameter to configure an area so that two different passcodes are required to disarm the area when it is Master Armed. Both passcodes must be assigned to an Authority Level with Passcode Disarm authority in the same area.
The steps below show how to disarm an area that is Master Armed with the A# Two Man Rule set to Yes.

1. The first user enters his passcode.
2. The system displays a prompt for a second passcode and begins a ‘second passcode delay’ equal to the Exit Delay programmed for the area.
3. The second user enters their passcode. The second passcode must be different than the first passcode.
4. The area is disarmed.

If the first passcode is entered during entry delay and the second user does not enter their passcode before the delay expires an alarm event occurs.
If entry delay **did not** start before the first passcode was entered and the second user does not enter their passcode before the delay expires, the Two Man Rule resets. The first user must reenter their passcode.
If there is an active alarm (alarm is sounding) in the area, entering the first passcode silences the alarm but **does not disarm** the area. The system requests the second passcode. Entering the second passcode disarms the area.

Additional Configuration Requirements:
Users must be assigned to an Authority Level with **L## Passcode Disarm** authority in the same area.
Keypads assigned to an area with the **A# Two Man Rule** set to **Yes** must be configured for Area Wide Scope (**CC# Scope** set to **Area**).
When the **A# Two Man Rule** set to **Yes** no keypads in the system can be assigned to Panel Wide Scope (**CC# Scope** must not be set to **Panel Wide**).
When the **A# Two Man Rule** set to **Yes** no keypads in the system with Account Wide or Custom Scope (**CC# Scope** set to **Account** or **Custom**) can include an area with **A# Two Man Rule** set to **Yes** in their scope.
Set **A# Early Ambush** to **No** for areas with the **A# Two Man Rule** set to **Yes**.

Notice!
Failure to follow the additional configuration requirements shown above will result in unintended system behavior.
The D720 Keypad does not support the Two-Man Rule feature.
The Two-Man Rule feature is not allowed for use in SIA CP-01 compliant installations. Consult the local authority having jurisdiction (AHJ) for proper usage. Refer to your control panel's entry guide for programming information.

2.3.2 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.

2.3.3 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.

2.3.4 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.

2.3.5 Single RPS Connection

– Only one connection to RPS can be made. RPS does not notify you if you are already in a connection.

2.3.6 Area Assigned

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

2.3.7 COMMAND 7 and COMMAND 9

– Bosch recommends that COMMAND 7 and COMMAND 9 be configured to not require a passcode. When an alarm is sounding, any passcode entry for any command will silence all alarms in all areas in which the user has authority.
– If a low-priority alarm is within its abort window and the alarm bell timer expires, the keypad annunciation will persist unexpectedly beyond the bell timeout. The keypad must be manually silenced with a valid passcode.

2.4 Support

2.4.1 Literature

Description	Part Number
D9412GV4/D7412GV4/D7212GV4 Program Entry Guide	F01U218312
D9412GV4/D7412GV4/D7212GV4 Program Record Sheet	F01U214958
D9412GV4/D7412GV4/D7212GV4 Operation and Installation Guide	F01U266054
D9412GV4/D7412GV4/D7212GV4 Approved Applications Compliance Guide	F01U266055
D9412GV4/D7412GV4/D7212GV4 UL Installation Guide	F01U266058

Table 2.1: Supporting Literature for GV4 Series with Firmware Version 1.00 and Later

2.4.2 RPS

http://products.boschsecurity.us/en/TAMS/products/bxp/SKU259512474745035999243621131-CATMfd62a57bdcda5b98fd2b359b463d9b6c.

2.4.3 Firmware Update

If required, update the panel firmware with the RPS Firmware Update wizard using the following connections and hardware:

- Enhanced Direct – DX4010V2 or DX4010i
- Network – B420, DX4020, or ITS-DX4020-G
- IP Direct – B420 or DX4020

To install the latest firmware updates via RPS software, go to the following web address: http://products.boschsecurity.us/en/TAMS/products/bxp/SKU259512474745035999243621131-CATMfd62a57bdcda5b98fd2b359b463d9b6c.
Install RPS software to install remote firmware updates for GV4 Series control panels.

3 Version 1.00

3.1 New

3.1.1 Remote Firmware Update

– GV4 Series control panels include the support of remote firmware updating via v5.14 or later. Only the panel firmware can be updated remotely. The control panel is not operational during firmware updates. All RPS connections are considered remote connections.

Local Authorization for Remote Firmware Update

– GV4 Series control panels include support for a control panel option to require local authorization for a remote firmware upgrade. This option is modified via RPS only.
– When the local authorization option is enabled, only a user with the Firmware Update Authority enabled can authorize the update.
– The Firmware Update Authorization command is in option in the Service menu (9-9-Ent). The Service menu is available from any text keypad.
– Firmware Update Authorization can only be granted when the control panel is in an active RPS session via the network.
– Once Firmware Update Authorization is granted, RPS disconnects and the control panel begins the update.

Preconditions

– When the Reset Switch option is enabled, and the local authorization is required, the control panel will not update the firmware until local authorization is granted (no troubles).
– The panel must be running normally, AC Power must be present, and the battery fully charged. Firmware updates will not be initiated by RPS if a power issue exists.
– Remote update will not be executed if the control panel is armed.

3.1.2 Automation/Integration Protocol

– GV4 Series control panels allow Automation software access to new GV4 features. These enhanced commands allow Automation software to connect to a control panel to query the panels alarm status, sensor status, as well as manage some user credential information.
– The GV4 Series control panels restrict Automation access to panel configuration by limiting read/write commands to user passcodes, authority levels, keyfob IDs, Sked Enable, Point’s Name Text, Area Name’s Text, etc.
– The GV4 Series control panels can support one of three possible network communication modules for Automation support; SDI Address 80, SDI2 Address 1, SDI2 Address 2. Only one automation link is allowed at a time.

3.1.3 Passcode Enter Function

Authentication

– The GV4 Series supports two methods of authentication for the operation of a Passcode Enter Function. These methods are passcode entry at a keypad or presentation of a credential at a D9210C door controller.
– Any keypad can have one of the following Passcode Enter Functions; **Arm/Disarm**, **Cycle Relay**, **Cycle Door (Door Access and Control)**, and **Auto Re-arm**.

Dual Authentication

- Dual authentication requires a user to present both a credential to a D9210C door controller, and a passcode to be entered at an associated keypad.
- Dual authentication requires the passcode and credential of the same user to be presented within the time duration set in **Command Center > Dual Authentication Duration**.

Arm/Disarm

- The Arm/Disarm function changes all authorized areas in scope from disarm to master armed, or from any armed state to disarmed when **Passcode** and [ENT] is pressed.
- The control panel shall only arm areas where the user has **L# Passcode Arm** authority enabled and shall only disarm areas where the user has **L# Passcode Disarm** authority.

Cycle Relay

- The Cycles Relay command momentarily activates a preconfigured output when **Passcode** and [ENT] are pressed.
- A user must have a non-zero authority level in the keypads current area to perform the Cycle Relay Function.

Cycle Door (Door Access and Control)

- The Cycle Door Command was enhanced to perform all functions associated with Door Access. After a user is authenticated, the door cycles the striker, the current area disarms, and then a custom function executes.

Auto Re-arm Features

- The Auto Re-arm function is intended to be used on a keypad with area-wide scope to provide a facility with the ability to temporarily disarm the perimeter before automatically re-arming.
- This keypad is assigned to an area that contains a perimeter delay point. The user can exit the facility through this point
- The Auto-Re-arm function automatically restarts the exit delay for Master Arm if the authenticating user has **L# Passcode Arm** authority and the keypads current area is already armed at any state.

3.1.4 Number of Users

Previous G Series control panels delivered 249 passcodes and 996 credentials using a User and Sub-User method. GV4 Series control panels support a total of 1000 unique users, whereby “User 0” is the installer. Each system user now supports a Passcode, Credential, and Keyfob so that user activity is unique and detailed.

- The D9412GV4 can support up to 1000 users.
- The D7412GV4 can support up to 400 users.
- The D7212GV4 can support up to 100 users.
- Standard Users are numbered from 1 to 999.
- Any control panel user can be configured via the keypad using Command 5-6, or through the use of RPS.
- All standard D9412GV4 and D7412GV4 users can have an access credentials assigned with individual authority permissions. Sub-Users are not supported.
- All standard users can be assigned a wireless keyfob through RF Diagnostics or Command 56 on a keypad or through RPS.

Notice!

If RPS is used to add, replace, or remove any keyfobs, no keyfob-specific events will be generated. Only the **Parameters Changed** event will be logged.

3.1.5 SDI2 Support

The GV4 series control panel support two independent SDI busses on the main control panel. The SDI2 bus does not support SDI devices.

SDI2 Module Supervision

- When an SDI2 device fails supervision, a system fault is annunciated at the keypads indicating the individual device number.
- When a SDI2 bus Octo-input module, or an RF Receiver module is declared missing, then all points associated with those devices will also be declared missing.

SDI2 Module Tamper

- Most SDI2 bus devices have an optional tamper input to detect when the cover is opened or when the device is removed from its mount.
- Module tamper conditions reported by SDI2 bus modules will be annunciated on the keypads as a system fault and optionally sent to the central station as an event.

SDI2 Open Wire Detection

- The GV4 Series control panels support the SDI2 bus to detect open communication wires (SDI2 A+, SDI2 B-). This system fault is annunciated on the keypads and optionally reported to the central station.

3.1.6 B208 Octo-input Module

- The D9412GV4 supports up to 24 Octo-input modules. The D7412GV4 supports up to 7 Octo-input modules. The D7212GV4 supports up to 3 Octo-input modules. Each Octo-input module supports up to 8 configurable points.

3.1.7 B308 Octo-output Module

- The D9412GV4 supports up to 12 Octo-output modules. The D7412GV4 supports up to 6 Octo-output modules. The D7212GV4 supports up to 2 Octo-output modules. Each Octo-output module supports up to 8 configurable relays.

3.1.8 B520 Auxiliary Power Supply Module

- All GV4 Series control panels support up to 8 auxiliary 12V power supply modules.
- Each Auxiliary Power Supply module monitors AC, up to 2 batteries, over current status and tamper status. When detected, these conditions are annunciated at the keypads, reported to the central station, and viewable in the RPS diagnostic screen.

3.1.9 B420 Network Interface Module

- The GV4 Series control panels support up to two B420 modules on the SDI2 bus.

Notice!

The communication modules on the SDI2 bus must be B420's. The communication modules on the SDI bus can be either DX4020 or B420 modules. When the B420 is installed on the SDI bus, it emulates the DX4020 and is restricted to the functionality of the DX4020.

- Configuration data such as the module's host name, the DNS server address and encryption keys can be configured in the GV4 control panel using RPS or keypad programming. The control panel configures the B420 network interface modules automatically.
- By default, the control panel retrieves configuration information in a newly installed B420 network interface module. When changes are made in the control panel, they will be downloaded into the module.

– With DHCP enabled and a B420 network interface module installed, the control panel can automatically establish its IP address, register its host name, and identify the network gateway for internet or intranet access if available.

Notice!
DHCP is disabled, the IP address, subnet mask, and default gateway must be configured manually.

– With a gateway defined, the control panel can route network communication for central station events and RPS network sessions through the internet or a corporate intranet. If DHCP is enabled, then the gateway will be automatically assigned if available.
– With a DNS (Domain Name Server) address configured and a B420 installed, the control panel can dynamically find the IP addresses of central station receivers and the PC running RPS. If DHCP is enabled, then the DNS address will be automatically obtained.

3.1.10 B820 Inovonics Interface Module

– The GV4 Series control panel supports one B820 Inovonics Interface Module.
– RF devices such as wireless points, smoke detectors, wireless RF repeaters, and keyfobs can be added to the system through RPS or keypad enrollment menus.
– Wireless keyfobs allow a user to arm or disarm all authorized areas from anywhere in the facility.
– The keyfob arm command can force arm the system if the user's authority level allows both keyfob arming and force arming.
– An RF Diagnostics menu is provided to dynamically report the signal strength of wireless points and wireless RF repeaters so that they can be installed in an optimal position.
– All points available in the GV4 Series control panel can be configured to have a specified source so multiple bus technologies can be used simultaneously. Point sources include ZONEX, Wireless, On-Board, and Access.
– A function of the GV4 Series control panel allows the support of the Inovonics EchoStream EN1224 Four-button Multi-condition Belt Clip Pendant, and the EN1224-ON Four-button Multi-condition Belt Clip Pendant with On/Off capabilities.
– The GV4 Series control panels support the B820 Inovonics Interface Module on the SDI2 bus. The B820 Inovonics Interface Module is powered by Inovonics wireless mesh network technology, which ensures superior range, reliability, and scalability for commercial applications. Using a wide range of transmitters and repeaters, this proven technology provides flexibility and performance to meet the most stringent requirements.

RF Repeaters

– The GV4 Series control panel supports up to 8 RF repeater modules. Each module is individually powered and reports battery and AC status to the control panel.

3.1.11 Keypad Programming

Module Encryption Parameters (AES Encryption Key Size)

– Each B420 Ethernet Communications Module can independently and optionally support 128-bit AES Encryption for RPS and central station communication.

AES Encryption Key

– The ability to display, add, and modify the AES encryption key is available in both keypad programming and through RPS.

Points

– Point Index and Point Source assignments can be made or removed through Installer Keypad Tools.

Inovonics Interface Module Management

– A keypad Tools Menu provides a means to enroll or replace wireless devices on premises. This menu also allows the installer to manually enter the RFID of wireless devices.
– The GV4 series control panels limit the total number of wireless devices (not including repeaters) to 350.

Routing Parameters

– Through the use of the B420, DX4020, and ITS-DX4020-G Network Interface modules, the GV4 control panel routing options comprise 16 routes to 4 network receivers and 4 phone routes.
– When a SDI2 or SDI communication module is used in a central station reporting route, it is automatically supervised on its corresponding bus. Any loss of bus communication is annunciated on the keypads as a Missing Device and reported if possible.

Notice!

If a B420 Ethernet Communications Module used at SDI2 address 1 or SDI2 address 2 has been configured as an automation interface module, then that module can not be used for central station nor RPS communication.

Firmware Authorization

– If enabled, local authorization for control panel firmware updates can be granted through the Service User Menu. Accessed by pressing [9][9][ENTER] at a keypad.

View Service Bypass

– To facilitate system maintenance for the Service User, a special point bypass option is provided to remove selected points from service. The status of points in Service Bypass can be viewed through the View Service Bypass menu. Accessed by pressing [9][9] [ENTER] at a keypad.

Installer Menu

– When the Reset Switch is in the closed position, a D1260 series keypad on SDI address 8 and a D1255 keypad on SDI address 16 will be automatically enabled. One of they keypads can be used to access the Installers Menu with the Installers passcode.
– The Installers Menu has the following options: View Log, Print Log, Display Revision, Service Walk Test, Default Text, View Service Bypass, Tools Menu and authorize Firmware Update.

Tools Menu

– The Keypad Programming menu, introduced on the GV3 series control panels, is accessible through two methods. From the Service Menu, access the Tools Menu and then scroll through the options to find the Programming sub-menu. You can also access the Programming menu from within the Installer menu.
– The Tools Menu requires authentication by the Service Users passcode before use. This is enabled by default and cannot be change.
– The Tools Menu includes sub-menus for Keypad Programming, Service Bypass, RF Points, RF Repeaters, RF Diagnostics, and IP Diagnostics.
– RPS is not allowed to connect to the control panel when the Tools Menu is active on a keypad. Likewise, the Tools Menu cannot be activated when the control panel is involved in an RPS session.

Keypad Programming

– The keypad Programming menu provides a means for limited programming on the control panel. Keypad programming can be enabled/disabled from RPS.

RF Points

– The RF Points menu provides a means to Enroll, Replace, and Remove the RFID for wireless points.

RF Repeaters

– The RF Points menu provides a means to Add, Replace, and Remove the RFID for RF repeater modules.

RF Diagnostics

The RF Diagnostics menu provides a means to view the status of RF Point and RF Repeaters.

Service Bypass

– Setting Service Bypass to YES disables a point. When Service Bypass is selected, the keypad displays the number of points that are Service Bypassed.

IP Diagnostics

– The IP Diagnostics menu is provides a mean to test each B420 Ethernet Communications Module to ensure that it can reach a specified network address on demand. This tool is provided to assist network administration personnel in troubleshooting any of the more advanced network module features. These diagnostic tests are not supported by the DX4020 Network Interface Module.

3.1.12 Event Log

– To better support various central stations communication formats, some actuating sources are represented as special User IDs. When actions are performed on the control panel by RPS, Key switches, or Automation software, the resulting events are logged with unique User IDs.
– All events stored in the control panel record the time and date including year. The range of years will be limited to 2010 through 2041.
– The event holds 1,023 events.

3.2 Corrections

3.3 Known Issues

3.3.1 Program Entry Guide Update

– Section *3.10.5 Arming Features* of the Program Entry Guide contains information for the A# Two Man Rule parameter that is incomplete. Use the following information in place of that found in the Program Entry Guide.

A# Two Man Rule

Default:	No
Selection:	Yes or No
Yes	Two different passcodes must be entered to disarm the area.
No	A single passcode can disarm the area.

The Two Man Rule feature is suitable for banks or other facilities that require a higher level of security to gain access to a vault or other protected area.

Use the parameter to configure an area so that two different passcodes are required to disarm the area when it is Master Armed. Both passcodes must be assigned to an Authority Level with Passcode Disarm authority in the same area.

The steps below show how to disarm an area that is Master Armed with the A# Two Man Rule set to Yes.

1. The first user enters his passcode.

2. The system displays a prompt for a second passcode and begins a ‘second passcode delay’ equal to the Exit Delay programmed for the area.
3. The second user enters their passcode. The second passcode must be different than the first passcode.
4. The area is disarmed.

If the first passcode is entered during entry delay and the second user does not enter their passcode before the delay expires an alarm event occurs.
If entry delay **did not** start before the first passcode was entered and the second user does not enter their passcode before the delay expires, the Two Man Rule resets. The first user must reenter their passcode.
If there is an active alarm (alarm is sounding) in the area, entering the first passcode silences the alarm but **does not disarm** the area. The system requests the second passcode. Entering the second passcode disarms the area.

Additional Configuration Requirements:
Users must be assigned to an Authority Level with **L## Passcode Disarm** authority in the same area.
Keypads assigned to an area with the **A# Two Man Rule** set to **Yes** must be configured for Area Wide Scope (**CC# Scope** set to **Area**).
When the **A# Two Man Rule** set to **Yes** no keypads in the system can be assigned to Panel Wide Scope (**CC# Scope** must not be set to **Panel Wide**).
When the **A# Two Man Rule** set to **Yes** no keypads in the system with Account Wide or Custom Scope (**CC# Scope** set to **Account** or **Custom**) can include an area with **A# Two Man Rule** set to **Yes** in their scope.
Set **A# Early Ambush** to **No** for areas with the **A# Two Man Rule** set to **Yes**.

Notice!
Failure to follow the additional configuration requirements shown above will result in unintended system behavior.

Notice!
The D720 Keypad does not support the Two-Man Rule feature.

Notice!
The Two-Man Rule feature is not allowed for use in SIA CP-01 compliant installations. Consult the local authority having jurisdiction (AHJ) for proper usage. Refer to your control panel’s entry guide for programming information.

3.3.2 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.

3.3.3 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.

3.3.4 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.

3.3.5 Single RPS Connection

– Only one connection to RPS can be made. RPS does not notify you if you are already in a connection.

3.3.6 Area Assigned

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

3.3.7 COMMAND 7 and COMMAND 9

– Bosch recommends that COMMAND 7 and COMMAND 9 be configured to not require a passcode. When an alarm is sounding, any passcode entry for any command will silence all alarms in all areas in which the user has authority.
– If a low-priority alarm is within its abort window and the alarm bell timer expires, the keypad annunciation will persist unexpectedly beyond the bell timeout. The keypad must be manually silenced with a valid passcode.

3.4 Support

3.4.1 Literature

Description	Part Number
D9412GV4/D7412GV4/D7212GV4 Program Entry Guide	F01U218312
D9412GV4/D7412GV4/D7212GV4 Program Record Sheet	F01U214958
D*9412GV4/D7412GV4/D7212GV4 Installation and Operation Guide*	F01U266054
D9412GV4/D7412GV4/D7212GV4 Approved Applications Compliance Guide	F01U266055
D9412GV4/D7412GV4/D7212GV4 UL Installation Guide	F01U266058

Table 3.1: Supporting Literature for GV4 Series with Firmware Version 1.00 and Later

3.4.2 RPS

http://products.boschsecurity.us/en/TAMS/products/bxp/SKU259512474745035999243621131-CATMfd62a57bdcda5b98fd2b359b463d9b6c.

3.4.3 Firmware Update

To install the latest firmware updates via RPS software, go to the following web address:
http://products.boschsecurity.us/en/TAMS/products/bxp/SKU259512474745035999243621131-CATMfd62a57bdcda5b98fd2b359b463d9b6c.
Install RPS software to install remote firmware updates for GV4 Series control panels.

4 Upgrading to a GV4 Series Control Panel

RPS Accounts Upgrade

RPS version 5.14 or newer is required to upgrade an existing G Series or GV2 Series Control Panel installation to a GV4 Series Control Panel. Refer to the RPS help files for the specific control panel for additional information on control panel 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.

Notice!

The D5200 Programmer is not compatible with the GV4 Series control panel.

– On-board Relays B (Terminal 7, labeled Alt Alarm) and C (Terminal 8, labeled SW Aux) are now installed in the factory. No supplemental installation or purchase is necessary to prepare these terminals for use.

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