Alliance Builder

User Manual

Document number/revision: **1054411A** (September 2005).

4. Limited warranty. GE SECURITY warrants that for one (1) year from the date of delivery of the Licensed Product (Software Warranty Period), the functions contained in the Software will be fit for their intended purpose as described in the applicable Documentation from GE SECURITY, and will conform in all material respects to the specifications stated in such Documentation. GE SECURITY does not warrant that the operation of the Software will be uninterrupted or error-free. GE SECURITY does warrant that the media on which the Software is furnished will be free from defects in materials and workmanship under normal use for a period of thirty (30) days from the date of delivery (Media Warranty Period). Except as specifically provided therein, any other software and any hardware furnished with or accompanying the Software is not warranted by GE SECURITY. Your exclusive remedy under this limited warranty for nonconforming Software shall be repair or replacement of the Software, in the sole discretion of GE SECURITY. To obtain a repair or replacement of nonconforming Software, contact GE SECURITY Customer Service toll free at 888-GESECURity or online at `www.gesecurity.com` during the Software Warranty Period. Your exclusive remedy under this limited warranty for defective media is replacement of the defective media. To receive replacement media under this limited warranty, return the defective media to Supplier during the Media Warranty Period, with proof of payment.

EXCEPT AS EXPRESSLY PROVIDED ABOVE, THE LICENSED PRODUCT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND, EXCEPT AS EXPRESSLY PROVIDED ABOVE, YOU ASSUME THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LICENSED PRODUCT.

5. Limitation of liability. GE SECURITY'S SOLE OBLIGATION OR LIABILITY UNDER THIS AGREEMENT IS THE REPAIR OR REPLACEMENT OF NONCONFORMING SOFTWARE AND/OR DEFECTIVE MEDIA ACCORDING TO THE LIMITED WARRANTY ABOVE. IN NO EVENT WILL GE SECURITY BE LIABLE FOR ANY DAMAGES, WHETHER CONSEQUENTIAL, INCIDENTAL, OR INDIRECT, NOR FOR ANY LOSS OF DATA, LOSS OF PROFITS, OR LOST SAVINGS, ARISING OUT OF USE OF OR INABILITY TO USE THE SOFTWARE OR DOCUMENTATION (OR ANY HARDWARE FURNISHED WITH THE SOFTWARE), EVEN IF GE SECURITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, NOR FOR ANY CLAIM BY ANY THIRD PARTY.

6. General. Any hardware provided to You by GE SECURITY shall not be exported or reexported in violation of any export provisions of the United States or any other applicable jurisdiction. Any attempt to sublicense, assign, or transfer any of the rights, duties, or obligations hereunder shall be void. This Agreement shall be governed by and interpreted under the laws of the State of New York, United States of America, without regard to conflicts of law provisions. You hereby consent to the exclusive jurisdiction of the state and federal courts located in Multnomah County, Oregon, to resolve any disputes arising under or in connection with this Agreement, with venue in Portland, Oregon.

Restricted rights legend. The Licensed Product is provided with RESTRICTED RIGHTS. In the event the United States Government or an agency thereof is granted a license, the following additional terms apply: Restricted Computer Software, as defined in the Commercial Computer Software–Restricted Rights clause at Federal Acquisition Regulations 52.227-19, and the restrictions as provided in subparagraphs (c)(1) and (c)(2) thereof; and as applicable, the Government's rights to use, modify, reproduce, release, perform, display, or disclose the Software also are restricted as provided by paragraphs (b)(2) and (b)(3) of the Rights in Noncommercial Technical Data and Computer Software–Small Business Innovative Research (SBIR) Program clause at DFARS 252.227-7018.

The manufacturer of the Licensed Product is GE Security Inc., 12345 SW Leveton Drive, Tualatin, OR 97062.

YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT AND AGREE TO BE BOUND BY ITS TERMS. YOU FURTHER AGREE THAT THIS AGREEMENT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN YOU AND GE SECURITY, AND SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATION RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

Intended use

Use this product only for the purpose it was designed for; refer to the data sheet and user documentation. For the latest product information, contact your local supplier or visit us online at `www.gesecurity.com`.

Contents

Chapter 2. View tabs 35

Chapter 3. Alliance Builder tools 79

Preface

This is the GE *Alliance Builder User Manual*. This document includes an overview of the product and detailed instructions explaining:

- how to use the user interface; and
- what the programming features are.

There is also information describing how to contact technical support if you have questions or concerns.

To use this document effectively, you should have the following minimum qualifications:

- a basic knowledge of the Alliance system components; and
- a basic knowledge of programming access and intrusion control panels.

Read these instructions and all ancillary documentation entirely before installing or operating this product. The most current versions of this and related documentation may be found on our website.

Conventions used in this document

The following conventions are used in this document:

Bold	Menu items and buttons.
Italic	Emphasis of an instruction or point; special terms.
	File names, path names, windows, panes, tabs, fields, variables, and other GUI elements.
	Titles of books and various documents.
Blue italic	(Electronic version.) Hyperlinks to cross-references, related topics, and URL addresses.
`Monospace`	Text that displays on the computer screen.
	Programming or coding sequences.

Safety terms and symbols

These terms may appear in this manual:

CAUTION: *Cautions* identify conditions or practices that may result in damage to the equipment or other property.

WARNING: *Warnings* identify conditions or practices that could result in equipment damage or serious personal injury.

Chapter 1 Introduction

This chapter provides an overview of Alliance Builder.

In this chapter:

Alliance Builder overview

To make designing and programming security systems faster and easier, Alliance Builder employs standard Windows drag and drop functionality. The application automatically takes care of many of the difficulties normally associated with security design including addressing and numbering devices.

Use Alliance Builder to:

- Program and label system devices
- Provide a descriptive name to all system hardware
- Handle bus addressing
- Configure doors/elevators
- Apply all system limitation rules during configuration
- Visualize the system architecture
- Create a portable project file that details the configured architecture
- Provide an as-built report (see *As-built tool* on page 81) that includes:

  - Project summary
  - CSI specification
  - Brochure
  - System overview diagram
  - Installer wiring information
  - Bus layouts
  - Device manuals/data sheets
  - Point ID address summary
  - Wireless serial number summary
  - Video integration summary
  - Parts list
  - Battery calculations
  - Cable calculations
  - Wiring diagrams

Hardware requirements

Alliance Builder minimum requirements:

- 600 MHz Pentium 3 (or equivalent) CPU
- 256MB RAM
- 200MB hard drive space for all required software
- SVGA Monitor, 1024 x 768 resolution, 16-bit high color
- 101 Keyboard
- Mouse or trackball device
- Network card
- Video card that supports DX7

Software requirements

Alliance Builder minimum requirements:

- Windows 2000, or Windows XP Home/Professional operating system
- Sufficient Windows permissions to install all components

Alliance Builder supports the optional ability to export parts lists to Excel spreadsheets. One of the following applications must be installed to export Excel parts lists (without Excel, the parts list can still be exported to a CSV file):

- Excel 2000
- Excel XP
- Excel 2003

Product specific function limitations

The project design and programming options available in Alliance Builder are dependent on the control panel and software management program you select for your project. These products are selected when you create a new project or open an existing project. Your view of Alliance Builder will reflect the limitations of the products you select.

For example, if you select a control panel that does not support 4-door controller DGP devices, when you open the project in Alliance Builder the programming features for 4-door controllers will not be available. The status bar will have the door totals cancelled out and the 4- door controller DGP devices will not appear on the *System device* tree in the *System layout* tab.

To ensure you have all the programming features required by your system, be careful to select the appropriate control panel and software management program.

Control panel limitations

The Alliance control panels provide the features shown in *Table 1*.

Table 1. Control panel features

Feature	AL-4X17	AL-3017	AL-2017
Areas	16	8	4
Maximum number of zones	256	64	32
Number of 8-zone expanders supported directly on control panel	2	2	2
Maximum number of relays	255	255	255
Maximum number of doors	48	48	0
Maximum number of DGPs	15	15	15
Maximum number of system bus RAS devices	16	16	16
Default number of alarm groups	32	32	32
Default number of door groups	10	10	10
Default number of floor groups	10	10	0
Expandable memory support	Yes	Yes	No
Clock relay controllers support	Yes	Yes	Yes
Number of card holders	50	50	50
Number of users with names	50	50	50
Number of users with PIN	50	50	50
Access logged events	10	10	10
Alarm logged events	250	250	250
Onboard zones	16	8	8
Onboard relays (physical and virtual)	5	5	5

Alliance management software program limitations

The Alliance management software programs provide the features shown in *Table 2*

Table 2. Alliance management software programs

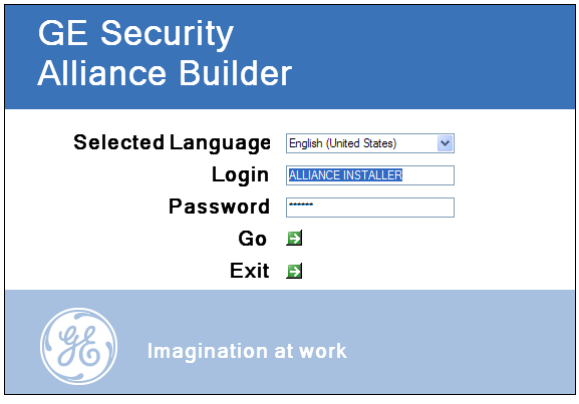
Feature	Alliance Professional	Alliance Enterprise
Number of work stations	1	4
Database engine	Borland BDE	Microsoft MSDE
TCP/IP LAN connectivity	Yes	Yes
Software licensing required	No	Yes
Maximum number of control panels	8	32
Management via dial-up	Yes	Yes
Reports	Yes	Yes
Bulk user update	Yes	No
Graphical maps	Yes	Yes
Video integration	Yes	Yes
Maximum number of DVMRs	2	8
Photo ID licensing required	No	Yes

Note: The firmware version in your control panel may also set limitations when you export your project to an Alliance software management program.

Initial log on

When you first execute the software, you access the *Log on* screen (*Figure 1*).

Figure 1. Log on screen



To log on the first time, use the following defaults:

Installer - ALLIANCE INSTALLER

Password - 998765

After you log on for the first time, we recommend that you change the default password. To change the password, do the following:

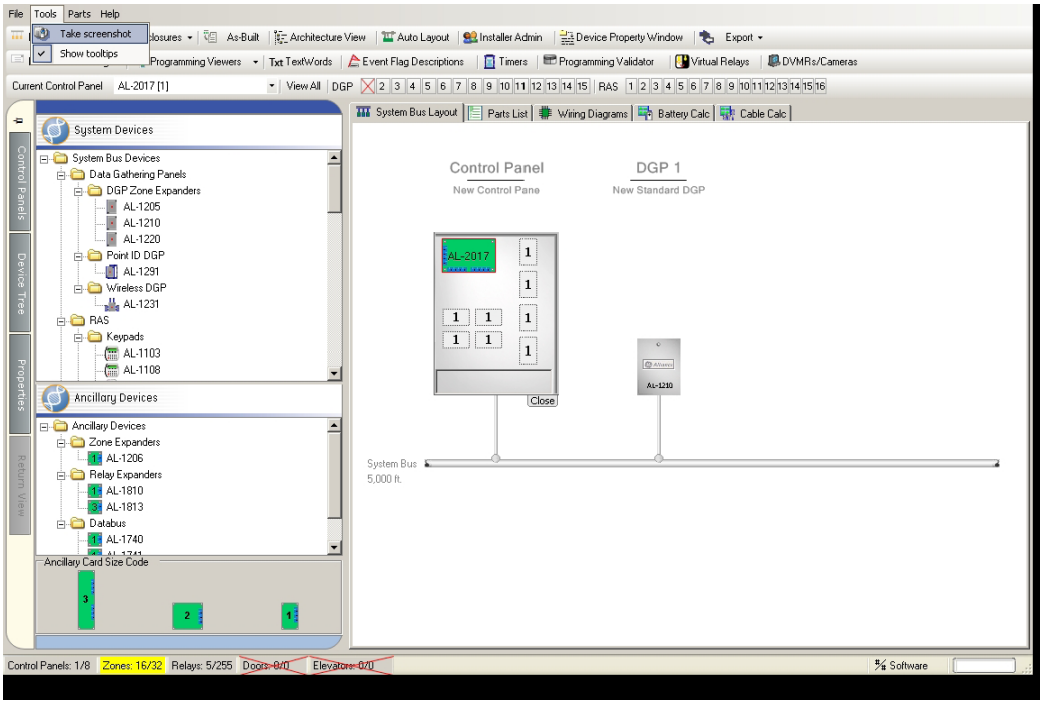
1. Select the *Installer administration* tool near the top of the application window.
2. Select the *Installers* tab in the *Installer administration* window.
3. Select **ALLIANCE INSTALLER** in the list of installers and click **Edit**.
4. Change the password and confirm password information in the *New/edit installer* window and click **OK**.
5. Click **Close** to exit the tool.

For more information, see *Installer administration tool* on page 85.

User interface

Alliance Builder has a user interface that is easy to use and follows standard practices. The user interface includes menus, toolbars, view tabs, status bars, and dialog boxes as shown in *Figure 2*

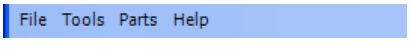
Figure 2. Alliance Builder interface



Menu bar

The menu bar shown in *Figure 3* is located at the top of the window.

Figure 3. Menu bar



File

The *File* menu includes the following options:

New project. Access the *New project selection* window to select the type of new project you want to create. The choices are:

- Standard project using the *New project* wizard *(*see *Create new projects* on page 39)
- Create a project based on an existing project or on a GE Security template (see *Create from template* on page 41).
- Import a project via the *Import project wizard (*see *Import/export projects* on page 28)

Close project. Closes the currently selected project and opens the *Project list* tab.

Save project. Saves the changes and updates that you have made to the current project.

Recent projects. Select a project to open from a list of recently created or updated projects.

Project properties. Access the *Alliance project properties* window to view contact numbers, customer information, and general information for the current project.

Logout. Log out without closing the application.

Exit. Closes the application.

Tools

The *Tools* menu provides the following options:

Take screenshot. Take a screenshot of the screen currently shown in Alliance Builder.

Show tooltips. Enable the blue bubble tooltips for Alliance Builder. This option does not impact the standard Windows tooltips.

Parts

The *Parts* menu includes the following options:

Recommended parts options. When you add certain devices to the project in the *System layout* tab, you have the option, through a dialog box, to also add recommended parts for the device. The parts you check are added to the project and

will appear on the parts list and in the As-built report. You can use this menu option to set the program to automatically check all the recommended parts for the devices you add to the layout.

Parts dialog behavior. Use this menu to indicate if you want Alliance Builder to recommend parts when you add devices to the project.

Export parts. Export the current project's parts list or export all supported parts to a file.

Import parts. Use this option to import parts lists to the *Parts list* tab. The *Import third party parts* dialog box can also be accessed through the *Parts list* tab. See *Import third party parts* on page 70 for details.

Organize third party parts. Use this dialog box to organize your third party parts list. See *Organize the parts tree* on page 71 for details.

Edit third party parts. Use this dialog box to edit third party parts. The *Third party parts* editor can also be accessed through the *Parts list* tab. See *Edit third party parts* on page 72 for details.

Help

The *Help* menu includes the following options:

Launch help. Opens this Help program

Visit Alliance on the web. Provides a link to Alliance information on the web.

About Alliance Builder. Provides copyright and historical information about Alliance Builder

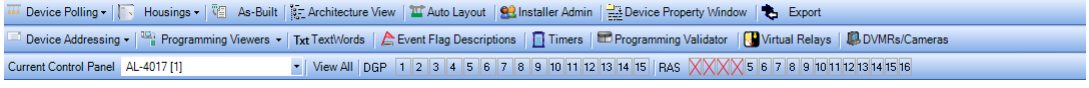
View tip of the day. Select this option if you want to see the tip of the day when you open Alliance Builder.

Enable all context tip. Select this option to enable all context tips.

Toolbar

The toolbar is located below the menu bar at the top of the program window (*Figure 4*). Click an icon on the toolbar as a shortcut to dialogs and actions. The toolbar only gives information and options for the currently selected control panel in the system layout. In systems with multiple control panels, you must ensure that the correct control panel is selected before using the toolbar (see *Current control panel tool* on page 109).

Figure 4. Toolbar



Alliance Builder tools

The top row of tools are used for programming functions that are not downloaded to the control panel. These tools include:

- *Device polling tool* on page 80
- *Enclosures tool* on page 80
- *As-built tool* on page 81
- *Architecture view tool* on page 84
- *Auto layout tool* on page 84
- *Installer administration tool* on page 85
- *Device property window tool* on page 89
- *Export tool* on page 90

Panel/device tools

The bottom two rows of tools are used for programming functions that will be downloaded to the control panel. These tools include:

View tabs

The view tabs are located below the toolbar and to the right of the left pane interface. *Figure 5* shows the view tabs as they appear when a project is open. In this view the *Project list* tab is hidden.

Figure 5. View tabs

The tabs include:

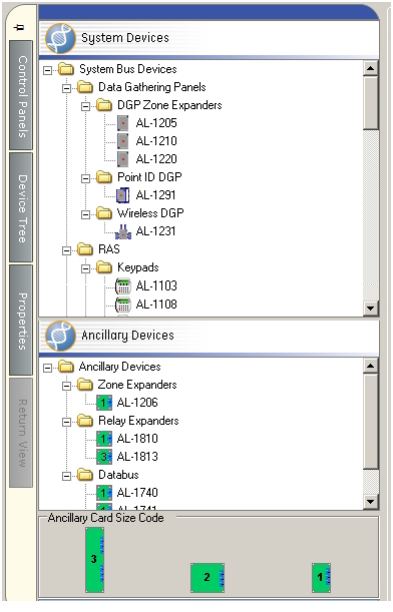
- *Project list tab* on page 36
- *System bus layout tab* on page 44
  - *Local bus layout tab* on page 58
  - *Control panel programming tab* on page 62
- *Parts list tab* on page 67
- *Wiring diagrams tab* on page 74
- *Battery calculation tab* on page 75
- *Cable calculation tab* on page 77

When you open Alliance Builder, the *Project list* tab will be active. To enable the other view tabs, you must select a project on the list or create a new project (see *Project list tab* on page 36). After you select or create a project, the *System bus layout* tab will open and populate with the information for the selected project and the *Project list* tab will be hidden. The *System bus layout* tab is a multilevel tab. From the System bus layout you can invoke the *Local bus layout* tab or the *Control panel programming* tab (see *System bus layout tab* on page 44).

Left pane interface

The information available through the left pane interface (*Figure 6*) is determined by the active view tab.

Figure 6. Left pane



The tabs to the left of the interface access the following information:

Control panels. A tree of the control panels currently in the project. See *Control panel tab* on page 46.

Device tree. A tree of available devices (will change when you activate a view tab).

Properties. A tree of the device properties (will change when you activate a view tab)

Return view. Returns you to the *System bus layout* tab from the *Local bus layout* tab or the *Control panel programming* tab.

When you select a view tab, the left pane interface will activate the tabs used for that view tab and populate with the appropriate information. Any left pane tabs that are not active for the selected view tab will be grayed out. See the specific view tab topic for information for the left pane interface for that tab.

Status bar

The status bar (*Figure 7*), located at the bottom of the program window, provides a running summary of the total number of various project capabilities for the currently selected control panel and the maximum number allowed in a system.

Figure 7. Status bar

The status bar is provided as a read-only feature and the information is automatically generated by Alliance Builder to reflect the present state of the system. The following information is included:

Control panel. Number used/maximum number allowed

Zones. Number used/maximum number allowed

Relays. Number used/maximum number allowed

Doors. Number used/maximum number allowed

Elevators. Number used/maximum number allowed

As devices are added or removed from the system, the following colors indicate the state of the project capabilities on the status bar.

Gray. This is the standard state for an attribute.

Blue. The attribute's numbers have changed.

Yellow. Over half the attribute's maximum allowed number is used. (50% maximum))

Red. The attribute is nearing the maximum number allowed. (90% maximum)

Black. The attribute is at the maximum number allowed and cannot be expanded. (100% maximum)

Icons

Icons are used in Alliance Builder to indicate programming features. The icons are used in the tool bars, view tabs and property programming trees to give visual clues to what is being programmed and how the programming features interact in Alliance programming.

Property programming

Property programming is accessed through property trees located in several areas of Alliance Builder. Most property programming is done through the *System bus layout* tab for specific device properties and through the *Control panel programming* tab for project-wide properties.

You can change the value of most properties. However, some properties are set automatically for you by Alliance Builder and cannot be changed. When a property is selected, a gray color indicates the property is read-only and cannot be changed, while a black color indicates a property that can be changed.

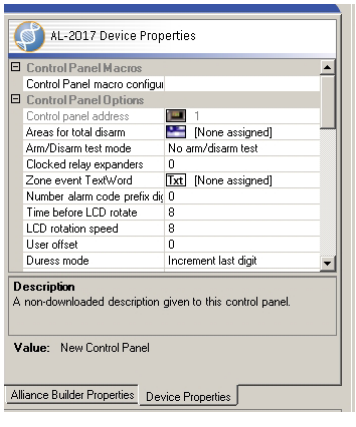
There are two lists of properties:

Alliance Builder properties. Alliance Builder properties are not downloaded to the control panel. These properties are defined by Alliance Builder and include the part number and the type of enclosure required. This information drives the *Required Alliance parts* list (see *Parts list tab* on page 67). Most Alliance Builder properties are read-only (grayed out) and cannot be changed.

Device properties. Device properties are downloaded to the control panel. These properties are set to defaults by Alliance Builder, but can be programmed as required for your application. In many cases, this will be a combined list of categories in order to provide access to all relevant properties for a given device.

*Figure 8*shows the *Device properties* tab open on the *System bus layout* tab.

Figure 8. Device properties tree



There are several methods provided to change property values. The type of programming feature and property value will determine the method used.

Double-click menus

Double-click a property name to access a drop-down navigation menu with various options to make programming faster and easier. A typical menu is shown in the following example:

What's this?

Create, assign, or view

Create and assign a new *X*.

Create and assign a new *X* and view in property window.

View assigned *X* in a property window.

Navigate to this *X*.

Reset or unassign

Reset to default.

Unassign the current value.

In the example shown, *X* is the name of the programming item. The specific drop-down menu choices are determined by the type of programming feature and property selected.

The navigation menus will direct you to the programming item you need. For example, if you have a RAS device and you want to assign event flag descriptions to a door event flag, you would:

- Double-click on the door event flag.
- Select *Create and assign a new event flag description and view in property window.*
- Alliance Builder will create a new event flag and a property window will appear with the item loaded.
- Click on the *Description* property and rename it.
- The event flag description in the property list on the tab will change to match the change you made in the property window.

Property editors

If you select a property name and there is a three-dot button to the right of the property value, click the button to access a property editor window. The property editor will give you the programming choices for the selected property. The programming choices are dynamic and will change depending on your project configuration. Only the programming choices that are available for your project are shown. To assign a programming option to the selected property, most editors provide a list of options that you can either double-click or select and click **OK**.

Property editors include:

Alarm groups editor. Assign an alarm group from the list. See also *Alarm groups* on page 188 for more information.

Event flag description. Assign an event flag description form the list. Event flag descriptions are programmed in the *Event flag descriptions tool* on page 101.

Hard/soft time zone editor. Assign an existing time zone from the list. Hard time zones and soft time zones are programmed in the *Control panel programming tab* on page 62.

Relay editor. Assign a relay from the list. Relays are programmed in the *Control panel programming tab* on page 62. See *Relays* on page 230 for more information.

Reporting class. The reporting class editor provides a tree of 8 reporting classes with 6 conditions for each. Select a condition and then check the applicable reporting boxes. See *Reporting classes* on page 221 for more information.

Text word editor. Assign a text word from the text word library. See *Text words* on page 271 for more information.

Floors editor. Assign an existing floor from the list. Floors are programmed in the *Control panel programming tab* on page 62.

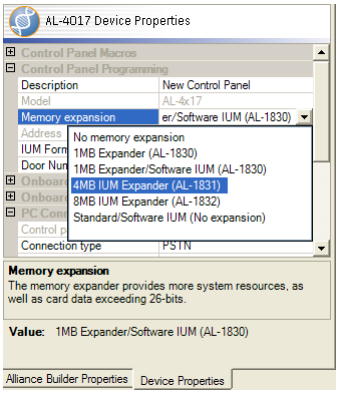
Macro editor. Assign macros for control panels and 4-door/elevator controllers. You can create new macros in this editor. See *Macro logic* on page 166 for more information.

Zones editor. Assign an existing zone from the list. Zones are programmed in the *Control panel programming tab* on page 62.

Arrow buttons

When you select some properties an arrow button is shown to the right of the property value. Some arrow buttons provide drop-down menus with programming choices for that property (*Figure 9*). The description displayed for the property name explains the implications of the programming choices. When options require a numeric value, the acceptable range and unit are provided to prevent you from entering an invalid value.

Figure 9. Property arrow menu

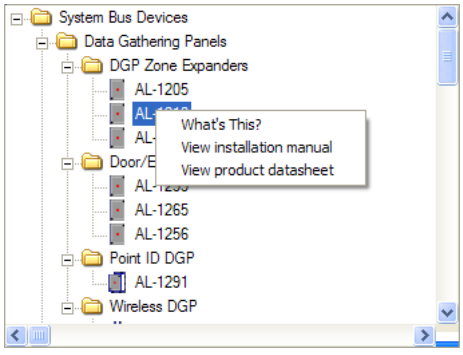


Some arrow buttons provide text boxes. These are used for property values such as descriptions of zones and other programming features that are not downloaded to the control panel. If there is default text in the box, you can overwrite the text to change it. There is a character length limit that you will not be able to exceed.

Device right-click menus

You can right-click devices on device trees and layout graphics to access drop-down menus. Right-click a device on a device tree to get the drop-down menu shown in *Figure 10*.

Figure 10. Right-click menu



Right-click any device on the system layout graphic to access a variety of menu options. The options available for each device depend on the type of device and how the device is programmed. Options include:

Remove all devices from the control panel. This option is only available for control panels. It allows you to remove all devices from the control panel.

Remove device. This option is not available for control panels. It allows you to remove the DGP or RAS device, its enclosure, and all devices connected to the DGP or RAS.

Click to view enclosure summary. Provides a read-only list of all devices/components found within this enclosure.

Click to view a summary for this control panel. This option is only available for control panels. It provides a brief describing and a read-only list of the control panel's capacities.

Device collections. This option provides the following choices:

- **Click for zone collection editor.** Opens the *Onboard zone setup* window. Use this window to program zones.

- **Click for relay collection editor**. Opens the *Onboard relay setup* window. Use this window to program relays.
- **Click for door collection editor.** Opens the *Intelligent door setup* window. Use this window to program door options.
- **Click to configure control panel macros.** Opens the *Control panel macro collection* editor. Use this editor to design up to 24 logic equations.
- **Click to configure 4-door/elevator controller macros.** Opens the *4-door/elevator controller macro collection* editor. Use this editor to design up to 48 logic equations.
- **Click to configure point ID devices.** Opens the *Point ID device configuration* window (see *Add devices to a point ID DGP* on page 54).
- **Click to configure wireless devices.** Opens the *Wireless transmitters setup* window (see *Add devices to a wireless DGP* on page 53).

Memory summary. Details limits for things such as alarm groups and door groups.

Creating projects

Before you begin a project in Alliance Builder you will need to have some basic information. This information includes both a general plan of the required elements of your project and specific company data.

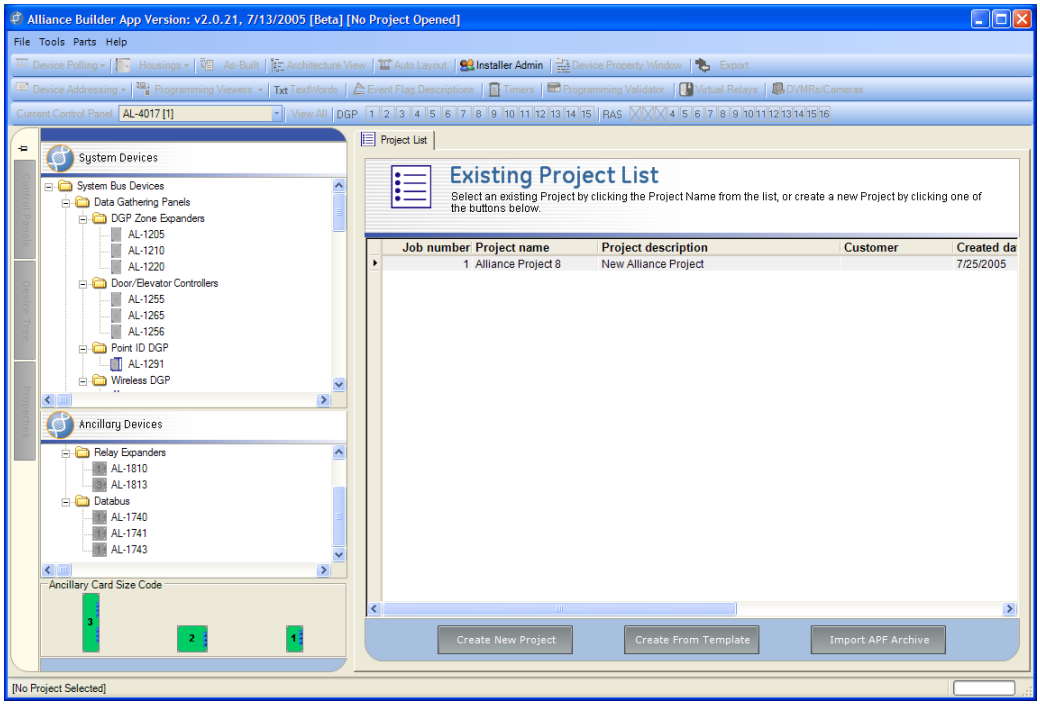
General project plan. To design a project in Alliance Builder you need to have a floor plan with the number of doors and elevators that will need control devices as well as an idea of the required location and type of control and sensor devices. This information will help determine the number of areas and zones needed for your project.

Company information. Alliance Builder requires company information when you create a project. This information will also be used on reports and forms generated by Alliance Builder. The information includes the company name, address, phone number, and contacts.

Project wizards and templates

After you log on to Alliance Builder, the program opens at the *Project list* tab (see *Project list tab* on page 36) shown in *Figure 11* on page 25.

Figure 11. Project list tab



To create a new project, click **Create new project**. This invokes the *Alliance project builder* wizard (see *Create new projects* on page 39) that will guide you through the necessary steps to create a new project. In the wizard, you will provide project information and select a control panel, enclosure, and other components that make up a basic Alliance system. Completing the wizard creates a new project containing all of the project information and components selected in the wizard and adds the project to the project list.

To create a new project using an existing project or a template, click **Create from template** (see *Create from template* on page 41). This invokes the *Template* wizard that will guide you through the necessary steps to create a new project. Using the *Template* wizard will make the process of programming a project much faster and easier. Choose the template that is closest to the project you need and the product selection and some of the properties programming will be done automatically. When you complete the wizard, the new project will be added to the project list.

When you select the new project from the project list, the *System bus layout* tab (see *System bus layout tab* on page 44) will open and populate the layout graphic with your new project components. Add any additional Alliance hardware you require to the system by dragging and dropping devices onto the layout from the device tree.

Basic programming sequence

After you have created a basic system using the project builder wizard or a template, we recommend you do the following steps to complete your project:

1. Program the control panel's Alliance Builder properties. See *Control panel* on page 160 and *System bus layout tab* on page 44.
2. Add any additional RAS devices needed to the system layout and program the devices Alliance Builder properties. The as-built description option is especially useful in larger systems to identify the device location in the project and ensure the devices are located at the proper entrances and exits. See *RAS (remote arming stations)* on page 112.
3. Program the DGP devices Alliance Builder properties. See *DGP (data gathering panels)* on page 120.
4. Select the control panel and enter control panel programming in system properties (memory format and IUM format). See *Control panel* on page 160.
5. Program the PC programming. (see *Control panel programming tab* on page 62)
6. Setup the areas needed for the project. (see *Areas* on page 178 and *Control panel programming tab* on page 62)
7. Program the central station configuration and communication options. (see *Central Station* on page 214 and *Control panel programming tab* on page 62)

To add the programming associated with zones, do the following:

1. Program the alarm groups. (see *Alarm groups* on page 188 and *Control panel programming tab* on page 62)
2. Program the time zones. (see *Hard time zones* on page 226 and *Control panel programming tab* on page 62)
3. Program the zones. (see *Zones* on page 236 and *Control panel programming tab* on page 62)

4. If the number of zones is not sufficient, add required DGP devices or zone expander devices. (see *System bus layout tab* on page 44)
5. Program the DGP Alliance Builder properties, then the zone programming for each DGP device. (see *System bus layout tab* on page 44)
6. Program the relays. (see *Relays* on page 230 and *Control panel programming tab* on page 62)
7. Add items from the GE parts list to ensure the number of zones equals the number of detection sensors. (see *Parts list tab* on page 67)
8. Add speakers and accessories. (see *Parts list tab* on page 67)

Import/export projects

All projects created in Alliance Builder have a unique identifier called a GUID (global unique identifier). This identifier provides a mechanism to synchronize projects while ensuring that two project numbers cannot point to the same deployed system. For example, if an installer creates a project and the project is later modified. When the project is imported back into Alliance Builder, the program will find the same identifier already exists in the database and will ask if the existing project should be replaced with the newer one.

Project archive file

The following files are contained in an Alliance Builder project archive:

Alliance Builder. Details all the project definitions that identify the part numbers, enclosure assignments, etc.

Panel defs. Control panel programming configuration.

Parts list.

Exporting process

Use the *Export* tool (see *Export tool* on page 90) to export a project to an archive file or to Alliance Professional.

Importing process

To import projects, do the following:

1. From the *Project list* tab (see *Project list tab* on page 36), click **Import APF archive** at the bottom of the tab. You can also use the menu bar (*Menu bar* on page 34)to select **File | New project**. In the *New project selection* window, select **Import APF archive** and click **OK**.
2. Browse to select the system configuration file you want to import.
3. Click **Open**.

You can not have two projects in Alliance Builder with the same project ID. If you try to import a project and the project ID already exists in Alliance Builder, a warning box will appear.

Recommended import/export strategy

To avoid adding programming time to the process, we recommend you follow these steps:

1. Design the entire project in Alliance Builder.
2. Export the project to an Alliance software management program.
3. Use the software management program to load the system to the control panel.
4. Check the system to see if additional programming is needed.
5. Make any required changes to the project in Alliance Builder.
6. Export the same project back to the software management program and load the system to the control panel.

Help

The Help Viewer provides a navigation pane with the following tabs:

Contents tab. Use the *Contents* tab to see a list of major categories of Help topics organized into books. Double-click a book to expand it into a list of topics. Click a topic to open it in the topic pane.

Index tab. Use the *Index* tab to see the Help index. Click an index entry to open a topic that contains information relating to the index entry. If more than one topic is found, a pop-up selection window with a list of related topics will appear. Click on a topic on the list to access that topic.

Search tab. Use the *Search* tab to search the Help topics.

Glossarytab. Use the *Glossary* tab to find definitions for words used in Alliance Builder.

You can **Hide** and **Show** the tabs by clicking the appropriate button

Copy a topic

In the topic pane of the Help Viewer, right-click inside the topic you want to copy, and select the **Select All option**.

Inside the topic, right-click again, and select **Copy**. This copies the topic to the clipboard.

Click the location in your document where you want the information to appear.

In the **Edit** menu, select **Paste**.

Note: *If you want to copy only part of a topic, select the part you want to copy, right-click the selection, and select **Copy**. Words that are links to other topics and step numbers are not copied to the Clipboard.*

Print a topic or book

Right-click the topic you want to print, and select **Print**.

Use the *Contents* tab to print all topics within a book. Right-click the book and select **Print**. In the *Print topics* window, select the **Print the selected heading and all subtopics** option and click **OK**.

Alliance system overview

The Alliance system combines access control and intrusion in one system that is made up of several different types of devices based around a control panel. The system components must be set-up and programmed to function together within particular parameters that are determined by the installer. Alliance systems can be very simple, with very few devices, or very large and complex with a wide range of devices. Because of this flexibility, it is important to understand the basic types of devices, how the system must be mapped, and how devices are addressed.

RAS (remote arming stations)

A RAS is a device, usually a keypad or card reader, that controls arming and disarming of areas within the Alliance system. A control panel can have up to 16 RAS devices connected on the system bus. When a RAS device is connected to a 4-door/elevator controller DGP on a local bus, up to four RAS devices are treated as a door by the Alliance system. A RAS device can be used to:

- Display zone, system and area status
- Specify the areas that can be accessed by the user
- Handle basic user access via a PIN
- Assign addresses to control panels
- Provide programming via menus
- Provide specialized programming functions

For more information on RAS programming options, see *RAS (remote arming stations)* on page 112.

RAS addressing

Most RAS devices have DIP switches that are used to set the RAS address on the RAS device. Be aware that although the control panel supports up to 16 RAS devices on the system bus and the system RAS address range is 1 to 16, the DIP switch address setting on the RAS device will be 0 to 15. You must subtract 1 from the system RAS address to get the correct DIP switch setting for the RAS device. For example, the first RAS device added to the system bus will be RAS 1 with a DIP switch setting of address 0.

For more information on RAS addressing and numbering, see *Numbering* on page 324.

DGP (data gathering panels)

A DGP, depending on the device type, can provide expansion capabilities, redundant databases, access control, zone monitoring, siren notification, and many other features. DGP devices connect to the control panel through the RS485 system bus. This system bus can extend up to a distance of 5,000 feet from the control panel, allowing the installer to distribute the system over a large area when needed and providing audible siren support to areas that would normally be difficult to cover.

The Alliance control panel supports up to 15 DGP devices. During system operation, the control panel will poll the DGP devices to obtain status information. Polling can be continuous or event based depending on your system's configuration. Despite their similar characteristics, control panels are not considered DGP devices.

For additional information on DGP devices and their programming options, see *DGP (data gathering panels)* on page 120.

DGP addressing

DGP addresses are set by using DIP switches on the devices. While most DGP devices have addresses that range from 1 to 15, some devices, such as the 4-door controller have addresses that range from 1 to 12. When setting the address on the DGP device, it is important to understand the Alliance addressing/numbering scheme to ensure that the address is set correctly (see *Numbering* on page 324). Before setting the address, refer to the specific device's installation instructions.

4-door/elevator controller DGP

The 4-door/elevator controllers provide intelligent doors (4-door controllers) and intelligent doors//floors (4-elevator controllers) control for the system through RTE (request-to-exit), antipassback, DOTL (door open too long), and access capabilities. The controller accommodates up to 4 RAS devices per door. The Alliance control panel can support up to 12 controllers, for a system maximum of 48 intelligent doors.

For more information see *4-door/elevator controllers* on page 123.

Point ID DGP

The Point ID DGP is capable of supervising a variety of addressable devices on a two-wire loop. A two-wire local bus supplies the power to the bus devices and provides command and

status information exchange between the DGP and bus devices. The DGP is designed to sit on the LAN of any existing configuration of Alliance products to expand the system with addressable devices. The control panel supports up to 15 addressable point ID DGP devices.

For more information see *Point ID DGP* on page 129.

Wireless DGP

The wireless DGP can be located up to 110 feet (335 meters) from the control panel. The DGP receives information from a range of compatible sensor types programmed into the DGP. It features spatial diversity to minimize wireless signal nulls or dead spots and has a nominal open-air receiving range of 1500 feet (460 meters). A repeater can also be used to eliminate dead spots.

The control panel supports up to 15 wireless DGP devices. DGP devices can be powered from the system data bus or through a remote auxiliary power supply. Fob buttons can be programmed for users to arm and disarm or to control relays. For example, to remotely open and close a garage door as well as arm or disarm an office security system.

The wireless DGP numbering follows normal DGP numbering. The actual zone numbers will depend on the address settings for the DGP. Sensors communicating with a wireless DGP will consume different numbers of zones, depending on the device category. Check the sensor's installation/programming manual to determine the number of zones that are consumed. For more information see *Wireless DGP* on page 132.

Expansion

Expansion modules provide a means of extending the zone (input) or relay (output) space. Expansion modules can be connected to the control panel via the expansion channel or they can be connected to a DGP device. The zone space consumed is dependent on the type of expansion module used.

Zones (inputs)

A zone provides input status to the system, either through a DGP or directly through the control panel. Zones are identified with a unique number. This number is assigned to the zone during installation. All reports or displays regarding a particular zone's status will use this unique number.

The Alliance 4X17 series control panels have 16 on board zones that are referred to as hard-wired zones because the zone (input) from a sensor is wired directly to the control panel via a series of connectors (see *Zones* on page 236).

Zone types and behavior

The zone type basically defines the behavior of the system based on the zone's input status or the actions taken when the input status transitions from one state to another. A zone's status is communicated to the input connection either by digital methods (in the case of a wireless DGP), or by analog (in the case of the control panel's hard-wired connection).

See *Zone types* on page 344 for a complete list of zone types.

Relays (outputs)

Relays follow the same numbering as zones (see *Numbering* on page 324). You can have a maximum of 16 relays per device, regardless of expanders. A relay can be inverted to reverse the active and normal state from normally open to normally on.

Relay programming

Events are mapped to relays through the following two methods:

- Macro logic programming applies a logical set of events to activate a relay output (depends on output selection). For example, a system event 24-hour alarm and particular zone event can be macro programmed to trigger a particular relay (see *Macro logic* on page 166).
- Relay programming uses a single event to trigger a relay output. A door event flag is the most common example (see *Relays* on page 230).

Chapter 2 View tabs

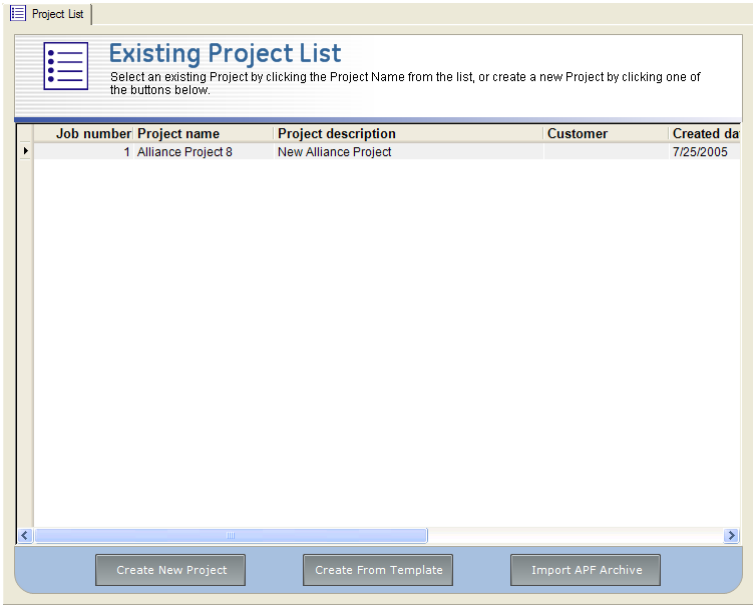
Use the view tabs to open, create, design, and program projects.

In this chapter:

Project list tab

Use the *Project list* tab (*Figure 12*) to create new projects and to access a list of current projects that includes the project name, the date it was last updated, the date it was created, and the installer.

Figure 12. Project list tab



The project list displayed is dependent on your installer type (see *Installer types tab* on page 87) and only contains the projects you have opened, created, or modified. If you want to access a project that is not on the list, use the Menu bar and select **File | Open Project** to access a list of all projects.

Open projects

To open a project, select the project name in the project list. Alliance Builder will open the project in the *System bus layout* tab.

Remove projects

When you remove a project from the project list, you will destroy all database entries and panel definitions for that project. All references to the project will be removed from Alliance Builder. If you want to retain files, you need to archive the files you want to keep before you remove a project.

To remove a project, do the following:

1. Right-click the project name on the list and select **Delete project** from the right-click menu.
2. In the *Confirm project delete* window, make sure the **Delete the project directory and all sub files/directories** check box is checked.
3. Click **Yes**.

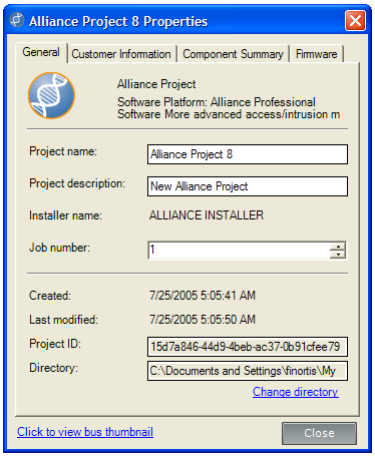
View project properties

Project properties can be viewed and some properties can be changed from the Project list. Any changes made to the properties will be reflected in the Project list.

To access project properties, do the following:

1. Right-click the project name on the list.
2. Select **Properties** from the right-click menu to open the *Project properties* window (*Figure 13*).

Figure 13. Project properties window



The *Project properties* window has the following tabs:

General. Provides general information that can be changed such as the project name, description, job number, and the project folder directory (use the *Change directory* link). Other information such as the installer name, the dates the project was created and last modified, and the project ID can not be changed.

Customer information . All of the customer information can be changed including the customer name, telephone number, and address.

Component summary. Provides a list of all components in the project. This component summary is a reflection of the projects system layout and can not be changed in this window.

Firmware. Provides information on the control panel firmware version. To change the version information, use the drop-down menu.

You can also use the **Click to view bus thumbnail** link to see the system layout graphic for the project.

Create new projects

We recommend that you create projects using the *Create from template* on page 41 option. If however, you want to create a new project without using a template, click **Create new project.** This accesses the *Alliance Builder* wizard. Use the **Back**, **Next**, and **Cancel** buttons at the bottom of the wizard window to navigate through the steps in *Table 3*.

Table 3. New project wizard

Welcome	Click **Next**.
Software platform	Select a software platform from the drop-down list. The part number, description, and attribute list are provided for the selected item. Use this information to ensure that the selected software platform is appropriate for your project. Click **Next**.
Project name and folder	Enter a name for your project that will be used for the project list and specify a project folder where all project files will be stored. Click **Next**.
Project information	Enter the project information specific to this project including the job ID and a project description if required. Click **Next**.
Customer information	Enter the customer information specific to this project including the customer name, phone number, and address. Click **Next**.
Control panel	Select the Alliance control panel for the project from the drop-down list. A list of attributes is provided for the selected panel. Use this information to ensure that the control panel selected is adequate for your project requirements. Click **Next**.
Firmware version	Select a firmware version from the drop-down menu. A list of attributes is provided for the selected version. Use this information to ensure the version selected is appropriate. Click **Next**.
Enclosure	Select the appropriate enclosure for the control panel from the drop-down list. A description and a graphical representation of various board layouts for the selected enclosure is provided. Click **Next**.
Transformer	Select a transformer from the drop-down menu. The selection available is driven by the device and enclosure already selected for the project. A description is provided for the selected transformer. Click **Next**.

Table 3. New project wizard (continued)

LCD keypad	Choose an LCD keypad to the project by selecting the **Select an LCD keypad** option and using the drop-down list. The *Part description* box provides a description of the keypad you select. Since all Alliance projects require an LCD keypad, if you select the **No LCD keypad** option, you must add a keypad to the system in the System layout tab. Click **Next**.
Required users	Select a memory module from the drop-down list. A list of attributes is provided for the selected module. Use this information to ensure that the selected module meet's your user requirements. Click **Next**.
PC connectivity options	Select the interface option required for your system. The *Part description* box provides a description of the selected option. Click **Next**.
Completed wizard	Click **Finish** to complete the new project creation and add the project to the project list.

Create from template

Click **Create from template** to create a new project based on the existing project or template that is closest to your application's requirements. Template choices are listed in *Templates* on page 42. The wizard directs you through the steps in *Table 4*:

Table 4. Create from template wizard

Welcome	Click **Next**.
Specify a project name/folder	Enter a name for your project that will be used for the project list and specify a project folder where all project files will be stored. Click **Next**.
Project information	Enter the project information specific to this project including the job ID and a project description if required. Click **Next**.
Enter customer information	Enter the customer information specific to this project including the customer name, phone number, and address. Click **Next**.
Template type	Select the type of source template you want to use for the project by choosing one of the following options: **Select a GE Security default program as a starting point for your new project.** If you select this option, do the following: • Click **Next**, the wizard provides a list of GE templates. • Select a template category from the drop-down list and select a template from the list of templates in that category. A device totals list will display for the selected template system as well as a brief overview description. See *Templates* on page 42 for a complete list of the available templates. • To get a list of the attributes for the control panel in the selected system, click **Tell me about this control panel**. The *Control panel summary* window details the control panel attributes and limits. • Click **Next** to accept the selected template. **Create a new project based on a previously designed project.** If you select this option, do the following: • Click **Next**, the wizard provides a list of existing projects. • Select a project from the list for your template and click **Next**.
Completed wizard	Click **Finish** to complete the wizard. The new project is added to the existing project list on the *Project List* tab.

Templates

The following templates are available through the *Create from template* wizard:

Easy

1. Basic intrusion using dial-up.
2. Basic intrusion using direct connect.
3. Expanded intrusion using direct connect.
4. DGP expanded intrusion using direct connect.
5. Intrusion using direct connect and 4 Smart RAS access.
6. Intrusion using direct connect and 4 Smart RAS access w/OC.
7. Intrusion using direct connect and a 4-Wiegand RAS access relay at the panel.

Moderate

1. Intrusion using direct connect and 4-Wiegand RAS access relay at the door.
2. Intrusion using direct connect and 4-door controller DGP with Smart readers.
3. Intrusion using direct connect and 4-door controller DGP with Wiegand readers.
4. Wireless intrusion using direct connect.
5. Point ID intrusion using direct connect.

Experienced

1. Intrusion using direct connect and 4-door controller DGP with Wiegand readers antipassback.
2. Intrusion using direct connect and 4-door control DGP with Smart readers antipassback.
3. Intrusion using direct connect and 4-elevator controller DGP with Smart readers.

Import APF archive

To import a project from an Alliance software management program or another Alliance Builder program, do the following:

1. Click **Import APF archive.**
2. Browse to select the system configuration file you want to import.
3. Click **Open**.

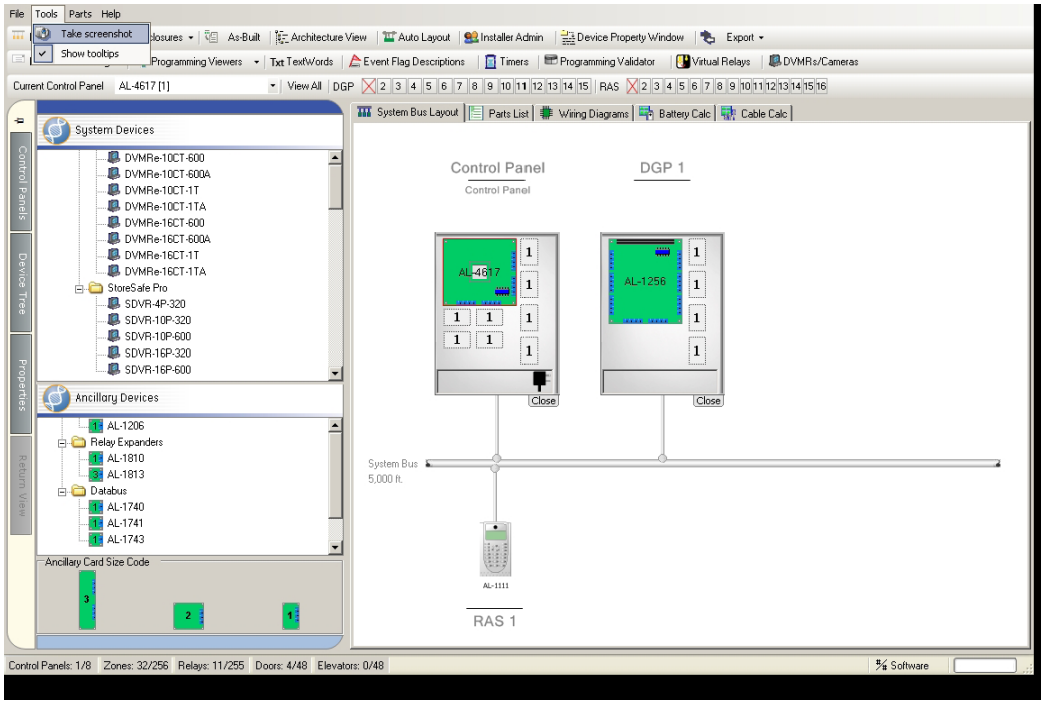
You can not have two projects in Alliance Builder with the same project ID. If you try to import a project and the project ID already exists in Alliance Builder, a warning box will appear.

See *Import/export projects* on page 28 for more information on importing and exporting projects.

System bus layout tab

The *System bus layout* tab (*Figure 14*) provides an interactive graphical representation of the system. Use this tab to design your project and to program the properties for the devices in your project.

Figure 14. System bus layout tab



The graphic in the layout will always represent the currently selected control panel. When you open a project, the layout will automatically populate with the information for that project and the programming options supported by that project will be active.

The *System bus layout* tab is a multilevel tab. From this tab you can invoke the following additional tabs:

Local bus layout tab. To invoke the *Local bus layout* tab, double-click a 4-door or 4-elevator control DGP device graphic on the *System bus layout*. The *Local bus layout* tab will populate with the information of the selected DGP device. See *Local bus layout tab* on page 58.

Control panel programming tab. To invoke the *Control panel programming* tab, double-click the control panel graphic on the *System bus layout* tab.The *Control panel programming* tab provides programming options for the control panel and the Alliance system. See *Control panel programming tab* on page 62.

Left pane tabs

The tabs on the left side of the left pane interface access the following:

Control panel tab. The *Control panel* tab contains a list of the control panels in the project.

Device tree tab. The *Device tree* tab contains a list of system devices and a list of ancillary devices that you can add to the system layout by dragging and dropping. Only those devices supported by the current control panel and your software platform will be available in the device tree.

Properties tab. The *Properties* tab includes both properties that are set by Alliance Builder and properties that you can change for the selected device.

Return view tab. The *Return view* tab returns you to the *System bus layout* tab from the *Local bus layout* tab or the *Control panel programming* tab.

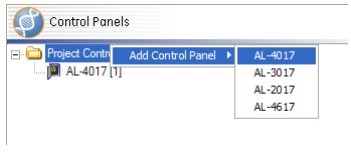
Control panel tab

Use the *Control panel* tab to see what control panels are currently in your project. You can also use the tab to add and delete control panels from your project, and view control panel documentation.

To add a control panel to the list, do the following:

1. Right-click the **Project control panels** folder.
2. Select a control panel from the list (*Figure 15*).

Figure 15. Control panel tree



3. Use the *Enclosure selection* dialog box to choose the appropriate enclosure and additional parts for the selected control panel and click **OK**.

The layout graphic will reflect the new control panel and its system bus.

To delete a control panel or to view control panel documentation, do the following:

1. Right-click the panel on the tree
2. Select one of the following options from the drop-down menu:
   - What's this?
   - View installation manual
   - View programming manual
   - View product datasheet
   - Delete control panel

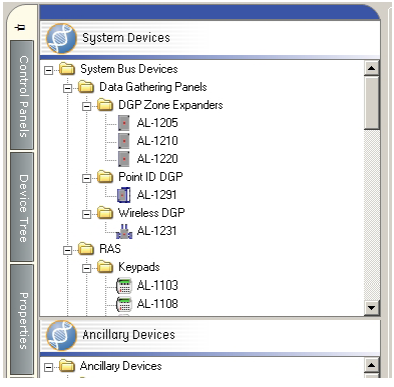
When you have more than one control panel in a project, you must always be aware of which control panel is currently selected. All programming options and graphics will reflect the currently selected control panel.

You cannot use this tab to change the currently selected control panel, you must use the *Current control panel tool* on page 109.

Add system devices

To add a system device to the layout graphic, open the *Device tree* tab (*Figure 16*). Click on the device in the system bus devices list and drag and drop it onto the layout graphic. This will place the device on the graphic and Alliance Builder will set the device address and default properties. Some devices require enclosures and other properties to be selected before they can be added to the layout. When you select one of these devices, a dialog box opens and you must supply the required information before the device is added to the layout.

Figure 16. Device tree tab



The rules regarding device placement include:

- A control panel must be on the system bus layout before any other device can be added.
- The first RAS device added to the system must be a keypad.
- As devices are added to the layout, the changes are reflected in the status bar at the bottom of the window. Devices can not be added to the layout if their addition will exceed the maximum number allowed for the system as indicated in the status bar (see *Status bar* on page 17).

Remove system devices

To remove a system device from the layout area, right-click the device and select *Remove device* from the right-click menu, or left-click the device to select it and hit the *Delete* key on your keyboard. Since a control panel is required for all systems, Alliance Builder will not allow you to remove the only control panel from the layout.

If you are removing a device, such as a DGP, that includes ancillary devices in the same enclosure, a confirmation box requires you to confirm the removal of all devices and the enclosure. You cannot remove the DGP device without removing all other devices in the enclosure and the enclosure itself.

After devices are removed, Alliance Builder will renumber and configure the remaining devices in the layout area and the status bar will reflect the those changes.

Use the *Auto layout tool* on page 84 to update the layout spacing after you remove devices.

Add ancillary devices

Ancillary devices are used to expand the functionality of your system. To access these devices, open the *Device tree* tab. Ancillary devices are categorized by their size as shown in the card size code area below the ancillary device list.

Installation of ancillary devices adheres to the following logic:

Occupied locations. Alliance Builder keeps track of installed devices and prohibits new devices from being placed in the same locations.

Physical fit. Alliance Builder searches to see if a location is available in the enclosure that matches the size of the device being placed.

Device type. Alliance Builder determines whether the type of ancillary device being added exceeds the number allowed under the system's electronic and firmware rules.

System input/output maximums. Alliance Builder will not allow placement of a device if the addition of the device will cause the system to exceed the maximum number of zones or relays allowed as shown in the status bar.

You can add an ancillary device to an existing enclosure or directly onto the system layout (size 1 and 2 devices only).

Add ancillary devices to an existing enclosure

Select the device in the ancillary device list and drag and drop it into an existing enclosure on the system layout. Each enclosure has a maximum number of ancillary devices that it can accommodate. This number depends not only on the number of card locations in the enclosure, but also on electronic and firmware limitations. Alliance Builder will not allow you to drop an ancillary device in an enclosure that does not have the proper space for it.

Add ancillary devices to the system bus

To add an ancillary device to the system bus, do the following:

1. Select the device in the ancillary device list and drag and drop it onto the system bus.
2. In the *Expander connection* window use the **Connect this expander to** drop-down menu to associate this device with a control panel. A description of the selected control panel is provided.
3. Click **OK** to close the window.
4. In the *Enclosure selection and recommended/default parts* window, select the enclosure for the device and select any recommended parts to associate with the device.
5. Click **OK** to close the window.

Remove ancillary devices

To remove ancillary devices from the system layout, right-click the device and select **Remove device** from the right-click menu, or left-click the device to select it and hit the **Delete** key on your keyboard. Only the ancillary device that is selected will be removed. Other devices in the same enclosure will not be affected.

View device properties

All devices in the layout have properties associated with them. To display the properties for a device that has been added to the layout, left-click the device. This will open the *Properties* tab. The description box below the properties list provides a brief description of a property when it is selected and the value box indicates what is currently programmed. You can also mouse over a property to view a brief description.

The following two lists of properties are provided:

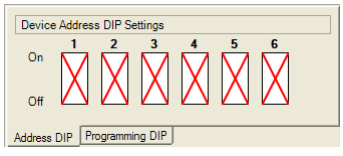
Alliance Builder properties. Alliance Builder properties are not downloaded to the control panel. These properties are defined by Alliance Builder and include the part number and the type of enclosure required. This information drives the required Alliance parts list (see *Parts list tab* on page 67). Most Alliance Builder properties are read-only (grayed out) and can not be changed.

Device properties. Device properties are downloaded to the control panel. These properties are set to defaults by Alliance Builder, but can be programmed as required for your application. In many cases this will be a combined list of categories in order to provide access to all relevant properties for a given device.

DIP switch tabs

The two tabs at the bottom of the device properties list provide graphical representations of the physical DIP switch settings required by some Alliance devices. If a device is selected that does not require DIP switch settings, the graphics will be disabled (*Figure 17*).

Figure 17. DIP switch tabs



Address DIP tab. Some Alliance devices have address DIP switches that need to be set on the device to reflect the device's address number on the system or local bus. When a device is added to the system layout, Alliance Builder automatically assigns an address to the device and sets the graphic on this tab to reflect that number. You can not change this graphic or the device number in the Alliance Builder properties list, and you must manually set the DIP switches on the device to match the graphic in Alliance Builder.

Programming DIP tab. Some Alliance devices have programming DIP switches that can be set based on the required functionality of the device, or other devices connected to the device. Some device programming DIP switches will be automatically set for a device based on system logic. To change a device's programming DIP switch settings, change the related property in the device properties list. The programming DIP switch graphic will change to reflect the programming in the device properties list. You must manually set the DIP switches on the device to match the graphic in Alliance Builder.

Change device properties

You can change the value of most device properties. However, some properties are set automatically for you by Alliance Builder and cannot be changed. When a property is selected, a gray color indicates the property is read-only and can not be changed, while a black color indicates a property that can be changed.

There are several methods provided to change property values. The type of programming feature and property value will determine the method used. See *Property programming* on page 18 for information on the following methods of changing properties:

- Double-click menus
- Property editor buttons
- Arrow buttons
- Right-click menus

Add battery requirements to devices

When you select a device on the layout graphic that has a power source, the property list will show a battery requirement option. Select this option to access the *Power distribution* window.

Power distribution window

Use this window to assign devices that draw power (power sinks) to the power source device you are programming. Drag the power sink device from the tree at the left and drop it below the power source device in the list on the right. To delete a power sink device from the right-hand list, select the device and click **Delete** on your keyboard.

In the *Power sinks* tree:

- All system bus devices are listed. Once a device from the tree has been assigned to a power source device, it cannot be assigned to any other power source.
- Power source devices on the tree will have an * by their names. They are shown on the tree to indicate the power sink devices assigned to them.
- All relays for the power source device are shown in angle brackets. When programming relays for the internal/external siren and strobe, the values will be higher since the current draw for these relays is higher.
- All zones for the power source device are shown in angle brackets.
- Use the *Custom entry* tree listing (the last item on the tree) to add anything that doesn't fall into the regular categories. This could include such things as Point ID devices.

Use the *Selected parameters* field to indicate the following information for the power source device:

- Description
- Standby current
- Alarm current
- Active current
- Duty cycle
- Relay inverted

The *Summary* field provides the following totals for the power source device:

- Total activation current (mA)
- Total base current (mA)
- Device power supply current (mA)

Default current editor

Use the **Edit zone sensor/relay current defaults** link at the bottom of the window to access the *Default current* editor. This editor allows you to specify default values for zones and relays. If you are using a similar set of sensors, this will prevent you from having to adjust all the similar items you assign to the power source device.

Select the item to edit from the drop-down menu and use the up/down arrows to set the following parameters:

- Default standby current
- Default alarm current
- Default active current

Click **Close** to save the defaults.

Parameter dialog box

Use the up/down arrows to set the following parameters:

- Required number of hours in standby
- Required number of minutes in alarm
- Required number of seconds in active.

In the **Required number of seconds active utility (badge rate)**, set the following parameters.

- Card activation
- Seconds
- Minutes
- Hours

Click **Apply** to generate the value for **Required number of seconds in active**.

Add devices to a wireless DGP

After you drag-and-drop a wireless DGP on the system layout, you can add and program wireless devices for the DGP.

To add devices to a wireless DGP, do the following:

1. Either right-click the wireless DGP graphic on the system layout and select **Device collections | Click to configure wireless devices** from the drop-down menu, or double-click the graphic. Both actions access the same *Wireless transmitter setup* window.
2. In the *Wireless transmitter setup* window, depending on the type of device you want, right-click the **Zone sensors, 16 total zones**, or **Key FOBs** folder on the tree.

3. Select **Add wireless zone transmitter** or **Add wireless key FOB**.
4. In the *Wireless selection* window, use the arrow button to access a drop-down list of devices and select a device from the list. Alliance Builder provides a description for the selected device in the *Description* field.
5. Select a 7-digit serial ID number by clicking **View all serial numbers**. This opens the *Wireless serial number* window that provides a list of all wireless devices currently in the project.
6. Click **Close** to exit this window and return to the *Wireless selection* window.
7. If you are adding a zone transmitter device, specify the number of zones by selecting one of the options in the *Specify the number of zones for this sensor* field. The number of zones is a reflection of the device type of the transmitter. If you are adding a key FOB device, use the *Specify FOB button functionality* field to specify if the buttons will be user, relay, or unused. If you choose relay, click the 3-dot button to access the *Relay editor* and double-click a relay from the list provided to assign it to the key FOB buttons.
8. Click **OK** to close the window and return to the *Wireless transmitter setup* window.

Program wireless device properties

You can also use the *Wireless transmitter setup* window to program certain properties for devices you have added to the tree. Click on the device in the tree to select it. Alliance Builder supplies most of the information shown to the right of the tree. You can, however, type in a description for the device in the *Description* box.

When you have finished adding and programming devices, click **Close** to exit the window.

Add devices to a point ID DGP

After you drag-and-drop a point ID DGP on the system layout, you can add and program point ID devices for the DGP.

To add devices to a point ID DGP, do the following:

1. Either right-click the point ID DGP graphic on the system layout and select **Device collections | Click to configure point ID devices** from the drop-down menu, or double-click the graphic. Both actions access the *Point ID configuration* window.

2. In the *Point ID configuration* window, right-click the **Total point ID devices** folder on the tree.
3. Select **Add new point ID device**.
4. In the *Point ID selection* window, use the arrow button to access a drop-down list of devices and select a device from the list.
5. The *Selected attributes* field shows a description, category, and zone/relay number for the selected device. Click **OK** to add the device.

Program point ID device properties

You can also use the *Point ID configuration* window to program properties for devices you have added to the tree. To program devices, click on the device in the tree to select it. Alliance Builder supplies most of the information shown on the *General* tab. You can, however, change the default value in the *Point ID address* field by clicking the 3-dot button and selecting an available address from the list provided. You can also type in a description for the device in the *Description* box.

If the device selected is a I/O device, two additional tabs are provided for programming zone and relay options. The *Zones* tab provides a drop-down menu to select one of the following for each zone:

Undefined. This is the default.

Double EOL. Double EOL (end-of-line) is a two-resistor configuration.

Single EOL. Single EOL (end-of-line) is a one-resistor configuration.

Zone is off. This indicates the zone not used.

The *Relay* tab provides a drop-down menu to select one of the following for each relay:

Undefined. This is the default.

Temporal. Siren output. Relay is off until event occurs.

Off/on. Relay is timed for on/off intervals.

On. Relay is always on (closed loop).

The *Relay* tab also provides a **Supervised** check box to program the relay as supervised. When you have finished adding and programming devices, click **Close** to exit the window.

Add cameras to a DVMR

After you have added a DVMR device to the system layout, you can add cameras to the device. double-click the DVMR device graphic on the layout. Alliance Builder will open the *DVMR setup* window. Use this window to specify DVMR parameters and to add and remove cameras.

Set DVMR parameters

Most of the *DVMR setup* field is read-only information supplied by Alliance Builder and dependent on the type of DVMR selected. You can overwrite the default text in the *Description* box and select a **Video standard** from a drop-down menu. LAN settings that can be programmed include a password, IP address, and Port number.

Click **View all IP addresses assigned to DVMRs** to open a window with a read-only list containing the number, description, and IP address for all DVMR devices in your project. Consult with your IT administration for network release details.

Cameras

The *Defined cameras for this DVMR* field provides a tree with the current camera information of the selected DVMR.

To add a camera, do the following:

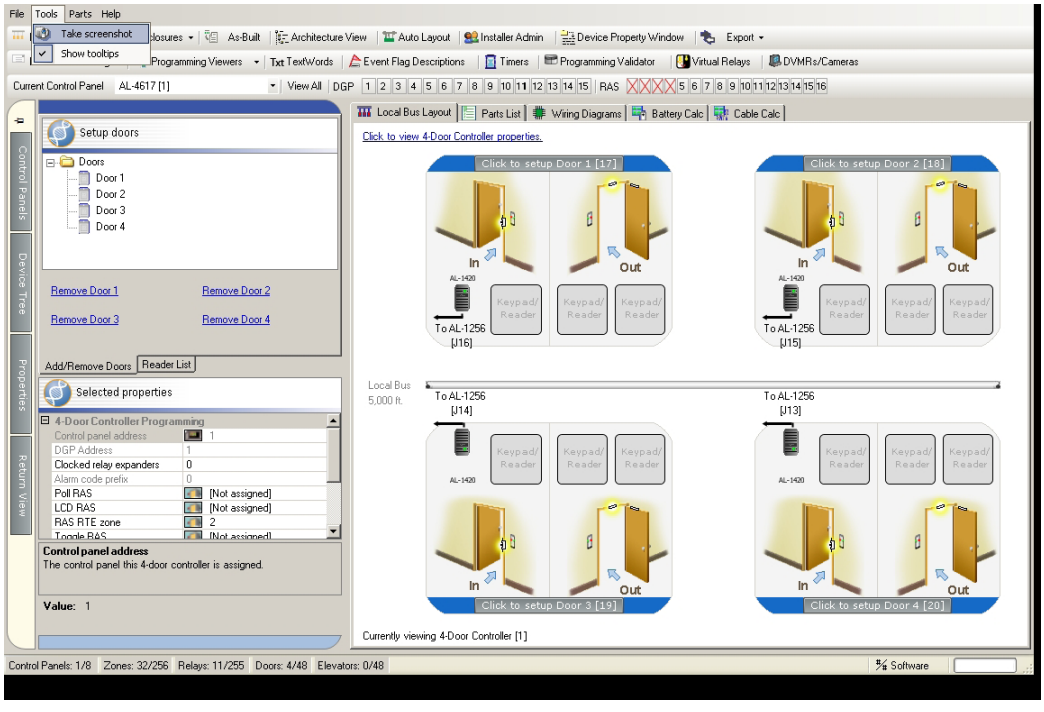
1. Right-click the **Cameras** folder.
2. Select the camera you want from the drop-down menu. The cameras are divided into several categories and your application should drive your selection.
3. The camera will be added to the *Defined cameras for this DVMR* tree and will be reflected in the Parts list.
4. To add a description to a camera, click the camera on the tree and overwrite the default text in the *Description* box in the *Selected camera* field. The other information in the *Selected camera* field is read-only and supplied by Alliance Builder.
5. To remove a camera from the tree, do the following:
6. Select the camera on the tree.
7. Right-click the camera and select **Remove camera**.

8. Click **Yes** in the confirmation box. The camera will be removed from the cameras tree and Parts list.
9. Click **Close** to exit the window.

Local bus layout tab

After you have added a 4-door or 4-elevator controller DGP on the *System bus layout* tab, double-click the DGP graphic to invoke the *Local bus layout* tab (Figure). The *Local bus layout* will populate with the information for the selected DGP.

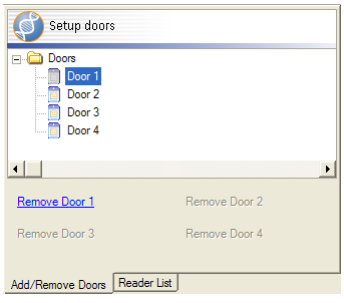
Figure 18. Local bus layout tab



Add doors to a 4-door controller

You can add and remove doors with card readers and keypads to the 4-door controller DGP on the *Local bus layout*. Select a door from the *Doors* list on the *Add/remove doors* tab and drag and drop it on the local bus graphic. To remove a door from the graphic, click the **Remove door** option for the door number you want to remove (*Figure 19*).

Figure 19. Add/remove doors



Card readers and keypads

To add local bus devices to a door, use the *Readers list* tab. Select a device from the device tree and drag and drop it in the door graphic. The first device on each door must be a card reader because the first device is connected to the reader keypad which is a wired device.

To view properties for local bus devices, click the device graphic. The Properties tab will populate with the properties for that device. Only the *Description* property can be changed, all other properties are read-only. You can overwrite the default text for the description property to identify the device for system programming.

If DIP switches are used on the device to set the device address, the graphic in the *Device address DIP settings* field will indicate how the DIP switches should be set. The graphic will be disabled if the device selected does not have DIP switches.

To remove a local bus device, right-click the device graphic and select **Remove device** from the list.

Program DGP properties

Although basic DGP programming for the 4-door controller can be done from the *System bus layout* tab, you can also access the same programming from the *Local bus layout* tab. Use the **Click to view 4-door controller properties** link at the top of the local bus graphic to populate the selected properties options with information for the DGP. Use the methods detailed in *Property programming* on page 18 to program the options.

Program door properties

Use the **Click to setup door** link at the top of each door graphic to program door properties for each door. Use the methods detailed in *Property programming* on page 18 to program the options. If you need more information about programming options, see *Doors* on page 138.

When you are finished adding and programming doors and devices to the DGP, click **Return view** on the left pane to return to the system layout graphic.

Add elevators to a 4-elevator controller

You can add doors/elevators with card readers and keypads to the DGP on the *Local bus layout* tab. Select a door/elevator from the *Doors/elevators list* on the *Add/remove doors* tab and drag and drop it on the *Local bus layout* graphic. To remove a door/elevator from the graphic, click **Remove door/elevator** for the number you want to remove.

Card readers and keypads

To add local bus devices to a door/elevator, use the *Readers list* tab. Select a device from the device tree and drag and drop it in the graphic. Note that the first device on each door/elevator must be a card reader.

To view properties for local bus devices, click the device graphic. The *Properties* tab will populate with the properties for that device. Only the *Description* property can be changed, all other properties are read-only. You can overwrite the default text for the description property to identify the device for system programming.

If DIP switches are used on the device to set the device address, the graphic in the *Device address DIP settings* field will indicate how the DIP switches should be set. The graphic will be disabled if the device selected does not have DIP switches.

To remove a local bus device, right-click the device graphic and select **Remove device** from the list.

Program DGP properties

Although basic DGP programming for the 4-elevator controller can be done from the *System bus layout* tab, you can also access the same programming from the *Local bus layout* tab. Use the **Click to view 4-elevator controller properties** link at the top of the local bus graphic to populate the selected properties options with information for the DGP. Use the methods detailed in *Property programming* on page 18 to program the options.

Program door/elevator properties

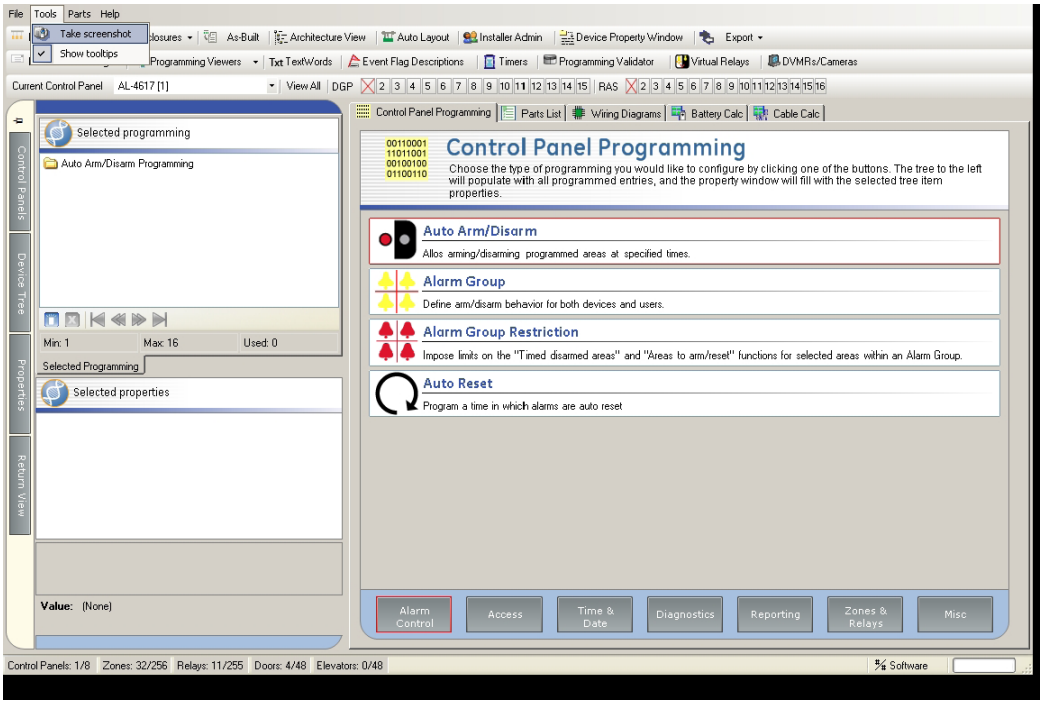
Use the **Click to setup Door** link at the top of each door graphic to program door properties for each door. Select either **Click to view Door properties** or **Click to view elevator properties** from the list. The selected properties options will populate with the information for that specific door or elevator. Use the methods detailed in *Property programming* on page 18 to program the options. If you need more information about programming options, see *Doors* on page 138 and *Elevator programming options* on page 127.

When you are finished adding and programming doors and devices to the DGP, select the **Return view** tab on the left pane to return to the *System bus layout* tab.

Control panel programming tab

To access the *Control panel programming* tab (*Figure 20*), double-click the control panel graphic on the system bus layout. Use the *Control panel programming* tab to program most system programming features. The available features are accessed through category buttons at the bottom of the window.

Figure 20. Control panel programming tab



Click a category button to get a list of programming features for that category (see *Programming features* on page 63), then click a programming feature from the list. The tree in the *Selected programming* field will populate with all programming records for that feature. Select an item on the tree and the *Selected properties* field below the tree will fill with the selected item's properties.

To return to the *System bus layout* tab, select the *Return view* tab on the left pane.

Programming features

The following programming features are available:

Alarm control

Auto arm/disarm. This feature allows you to arm/disarm programmed areas at specified times. For more information, see *Automatic arm/disarm* on page 201.

Alarm group. Alarm groups are assigned to each RAS device in the system and dictate the areas the device has control over, the times the alarm group is valid, the menus that will be accessible, and the functionality that is supported by the RAS device. For more information, see *Alarm groups* on page 188.

Alarm group restrictions. Alarm group restrictions impose limits on the *Timed disarmed areas* and *Areas to arm/reset* functions for selected areas within an alarm group. For more information, see *Alarm group restrictions* on page 197.

Auto reset. Auto reset allows you to automatically reset alarms after a specified period of time. For more information, see *Automatic reset* on page 203.

Access

Areas. Areas define a physical space within a building to establish intrusion protection, through zones, and to tie those zones to RAS devices through alarm groups. For more information, see *Areas* on page 178.

Area links. Area links tie several areas together to create a common area. For more information, see *Area links programming* on page 184.

Regions. Regions are used in establishing boundaries within 4-door/elevator controllers. The system allows you to assign regions to both the IN and OUT readers on the 4-door/elevator controller. When a user is granted access at a door, the user is assigned that particular region. For more information, see *Regions* on page 186.

Bank vault areas. Bank vault areas are areas designated as high security requirements. The system will automatically arm all bank vault areas after a preset delay. For more information, see *Bank vault areas* on page 185.

Floor. Floors descriptions are used to identify floors within elevators during programming. They are not downloaded to the control panel.

Time and date

Hard time zones. Hard time zones define periods of time, including the time and of day and the day of the week and holidays that are typically used to allow or prevent certain actions from taking place. For more information, see *Hard time zones* on page 226.

Holidays. Holidays are used in conjunction with time zones in order to define additional access parameters. For more information, see *Holidays* on page 228.

Diagnostics

Next service call. This feature allows you to set a date for programmed text to display on the LCD arming station indicating that the next routine service call is due. For more information, see *Next service* on page 209.

Test call. The test call performs a regular interval report call to the central station to ensure that central station reporting is working and that no problems have occurred that would prevent it from reporting access and alarm events. For more information, see *Test call* on page 210.

Clock correction. The clock correction feature allows you to program a correction factor that compensates for a control panel clock that may be running slightly fast or slow. For more information, see *Doors* on page 138.

Battery test. The battery test tests the state of batteries connected to system bus devices. For more information, see *Battery test* on page 206.

Reporting

Central station configuration. The central station configuration defines the line account number, phone number, etc. For more in formation, see *Central Station* on page 214.

Central station communications. Central station communications defines how messages will be recorded and what medium will be used. For more information, see *Communication programming* on page 217.

Reporting class. Reporting classes let you specify what is reported in the event of an alarm. For more information, see *Reporting classes* on page 221.

Zones and relays

Zone. A zone, also known as an input, is typically a sensor wired either directly into the control panel, through a DGP, or through an expander board. For more information, see *Zones* on page 236.

Zone shunts. A zone shunt will bypass a zone for a specified period of time when the zone is in the active state. For more information, see *Zone shunts* on page 246.

Relay . Relays can be either physical relays attached to the control panel and relay expander boards, or logical relays used in macros. For more information, see *Relays* on page 230.

Soft time zones. Soft time zones, similar to system macros, are programmable logic that can be used to enable/disable certain actions. For more information, see *Soft time zones* on page 233.

Miscellaneous

Control panel options. Control panel options are a collection of options that will affect all related functionality in the system. For more information, see *Control panel options* on page 252

System event flags. System event flags deal with system-level events. When the specified conditions occur, the system will cause the programmed event flag to be raised. For more information, see *System event flags* on page 268.

Event flag description. Event flag descriptions are used to fully describe the meaning of the custom event flags. They should be used so that any installer can easily understand the purpose behind each event flag, especially when it comes to programmable logic (Macros). Event flag descriptions 1 to 16 are predefined and cannot be changed. For more information, see *Event Flags* on page 264.

Custom LCD message. The custom LCD message allows you to modify the text displayed on the RAS devices connected to the control panel. For more information, see *Custom LCD message* on page 263.

Text words. Text words are used to add descriptions to system components. These descriptions can be downloaded to the control panel. Up to 100 user-defined text words can be added to the text word library. Use the Text word tool to view the pre-defined library of text words. For more information, see *Text words* on page 271.

Selected programming field

The *Selected programming* field at the top of the left pane interface contains a tree of all of the selected feature's programmed records. For some programming features, such as Zones, Alliance Builder will populate the tree with all records required by the current project. These requirements reflect the devices currently on the system layout. Other types of features, such as Holidays, require you to add the records you need for the system using the **Add file** icon below the tree. Records you add to the tree can also be deleted using the **Delete** icon. Features that rely on Alliance Builder to supply the required records will have the add and delete icons disabled.

Selected properties field

When you select a record in the *Selected programming* field, the *Selected properties* field below the tree will fill with the programming properties for the selected record. The list indicates the property name on the left and the programming value on the right. When you select a property name on the list, a description of the property appears in the description box below the list, as well as the current value programmed for the property. Properties that cannot be changed, such as the control panel address, will be grayed out.

Property programming

You can change the value of most device properties. However, some properties are set automatically for you by Alliance Builder and cannot be changed. When a property is selected, a gray color indicates the property is read-only and can not be changed, while a black color indicates a property that can be changed.

There are several methods provided to change property values. The type of programming feature and property value will determine the method used. See *Property programming* on page 18 for information on the following methods of changing properties:

- Double-click menus
- Property editor buttons
- Arrow buttons
- Right-click menus

Parts list tab

Use the *Parts list* tab to view, edit, and print parts lists for your project. The tabs at the bottom of the pane provide access to the following three parts lists:

GE Security parts list. Required and optional GE parts

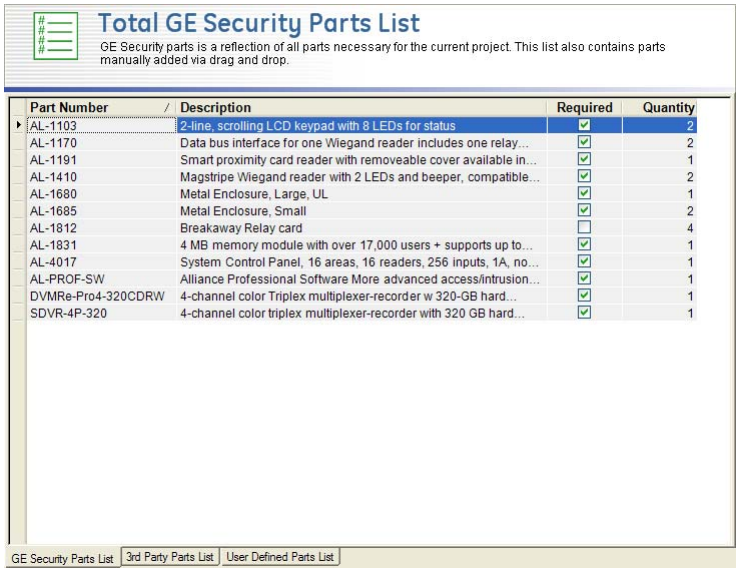
Third party parts list. Imported non-GE parts

User defined parts list. Text-only part information

GE Security parts list

The *GE Security parts list* tab (Figure) provides a list of required and optional GE parts. Alliance Builder automatically populates the list with the parts required by the project as shown in the System layout tab. GE parts not required by the system layout can be added from the GE parts tree in the left pane.

Figure 21. GE Security parts list



The parts list provides the following information:

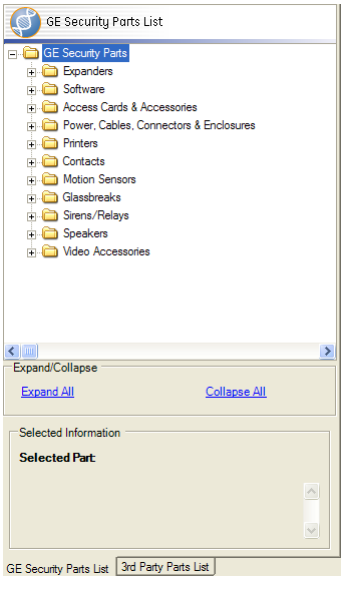
- Part number
- Description of the part
- Check box that indicates if the part is required by the project in the system layout (only parts that have been added to the system layout graphic are indicated as required parts)
- Quantity required

Add GE parts

To add an optional GE part to the parts list, do the following:

1. Select a part from the parts tree in the left pane interface (*Figure 22*). When a part is selected, a brief description of the part will display in the *Selected information* field.

Figure 22. GE parts tree



2. Drag and drop the part from the tree to the parts list. You can only add one part at a time, you can not drag and drop folders.

3. The parts list will reflect the change.

Alliance Builder will not change the system layout graphic to reflect GE optional parts added to the parts list. To change the system layout you must use the *System layout* tab.

To add required GE parts, do one of the following:

- Add the device in the *System bus layout* tab. Alliance Builder will update the parts list to reflect changes in the system layout.
- Or, right-click on the required check box of a part on the parts list to add a check to the box. The system layout will not be changed.

Remove GE parts

To remove an optional GE part, do one of the following:

- Select a part on the parts list (you can only remove one part number at a time) and hit the **Delete** key on your keyboard.
- Or, change the value in the *Quantity required* column to *0*.

To remove required GE parts, do one of the following:

- Remove the device in the *System bus layout* tab. Alliance Builder automatically updates the parts list to reflect changes to the system layout.
- Or, right-click the required check box to remove the check from the box and then hit the **Delete** key on your keyboard.
- Or, change the value in the *Quantity required* column to *0*.

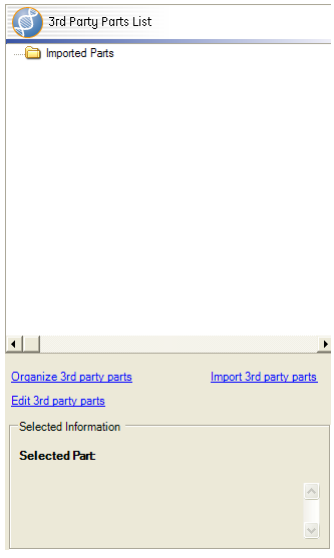
Third party parts list

The *Third party parts list* tab provides a list of parts with the following information:

- Part number
- Description of the part
- Quantity required

The left pane interface is used to store imported parts in a parts tree (*Figure 23*) that can be added to the parts list. The left pane also allows you to import part files, organize, and edit the parts tree.

Figure 23. Third party parts tree



Import third party parts

You can add parts to the parts tree by importing Excel files, text files (CSV), or clipboard text from your PC. To import the file or text, click **Import Third party parts** (*Figure 23*).

Select the source for the parts in the *Import Third party parts* dialog box.

If you select **Microsoft Excel file**, do the following:

1. In the *File browser* dialog box, indicate the location of the file you want to import and click **Open**.
2. Click **OK**.
3. In the *Parts import mapping* dialog box, select the appropriate part number and description columns.
4. Click **OK**.

The information from the source file is added to the parts tree and you can add it to the third party parts list.

If you select **Comma separated values text file (CSV)**, do the following:

1. Click **OK**.
2. In the *File browser* dialog box, indicate the location of the file you want to import.
3. Click **OK**.
4. In the *Parts import mapping* dialog box, select the appropriate part number and description columns.
5. Click **OK**.

The information from the source file is added to the parts tree and you can now add it to the third party parts list.

If you select **Windows clipboard (copy/paste)**, do the following:

1. Click **OK**. All information on your PC clipboard will be copied. Be sure only the appropriate text is on the clipboard.
2. In the *Parts import mapping* dialog box, select the appropriate part number and description columns.
3. Click **OK**.

The information from your clipboard is added to the parts tree and you can add it to the third party parts list.

Organize the parts tree

To make parts in the tree easier to find, you can organize the parts in folders and subfolders. However, to add parts from the parts tree to the parts list, you must open the folders and add the parts one at a time. You can not drag and drop folders from the parts tree to the parts list.

To organize the parts tree, do the following:

1. Click **Organize third party parts** (*Figure 23*).
2. To add a folder in the *Organize part list* dialog box, click on the node where you would like the folder to be placed, and click **Add folder**.
3. To remove a folder, select the folder and click **Delete folder**.
4. To move parts from one folder to another, select the item and drag and drop it in the new folder.

5. Click **Close** to exit the dialog box.

The changes made will be reflected in the *Third party parts tree* tab.

Edit third party parts

To change a part number or description for a part, do the following:

1. In the left pane, click **Edit third party parts** (*Figure 23*).
2. In the *Custom parts editor* dialog box, select and overwrite the part number or description.
3. To remove a part, select the part and hit the **Delete** key on your keyboard.
4. To add a part, click **Add a new part** and overwrite the default text in the part number and description columns.
5. Click **OK** to exit the dialog box.

Add third party parts to a project

To add a part, do the following:

1. Select a part from the parts tree. When a part is selected the description provided for that part will display in the *Selected information* field.
2. Drag and drop the part into the parts list. You can only add one part at a time, you can not drag and drop folders from the parts tree.

Remove third party parts from a project

To remove a part, do the following:

1. Select a part in the parts list. You can only remove one part number at a time.
2. Hit the **Delete** key on your keyboard.

User defined parts list

The *User defined parts list* tab provides a place to add any required additional text. The text box allows you to create a column of text that you can add, edit, and delete. Any information

added in the text box will print with the other parts lists and will be part of the As-built report. The left pane is not used and is not available from this tab.

To add an item, do the following:

1. Click **Add new item**.
2. Type the text in the new item line in the *Description* text box.

To edit an item, do the following:

1. Select the item line in the *Description* text box.
2. Type the new information in the item line.

To delete an item, do the following:

1. Select the item line in the *Description* text box.
2. Click **Delete selected item**.

Print the parts list

To print the parts list, use the *As-built tool* on page 81.

Wiring diagrams tab

The Wiring diagrams tab provides a technical point of reference for the configuration and wiring of all devices in your project. The diagrams will reflect your project settings and the programming you have completed in Alliance Builder. The diagrams include programming details such as:

- Zone names
- Relay names
- Door names
- Address and programming DIP switch settings.

You can also access wiring diagrams for all devices in your project by using the As-built tool. From the As-built tool you can choose to print the wiring diagrams in high or low resolution and you can request a zone, relay, and/or door index.

View wiring diagrams

You can only view one diagram at a time. Use the device tree in the left pane to select a device and the diagram for that device will appear. Only devices that are included in the system layout will be available in the device tree.

Save wiring diagrams as images

To save a wiring diagram as an image, right-click the device in the tree in the left pane and select **Save diagram to image**. Use the *Save as* box to select the type of image you want (Jpeg, Bitmap, GIF, or Png) and browse to the folder where you want the image saved.

Print wiring diagrams

To print the wiring diagrams, you must use the *As-built tool* on page 81.

Battery calculation tab

Use the Battery calculation tab to calculate the backup battery requirements for your project. Before doing the calculation, you must use the System layout tab to specify the following information for each device in your project containing a power supply:

- The required number of hours in standby
- The required number of minutes in alarm
- The required number of seconds in active

After you add this information in the System layout tab, click Calculate on the Battery calculation tab to start the battery calculation. The following system battery requirements will be calculated and shown in the *System battery requirements* field:

- Standby Amp-hours
- Alarm Amp-hours
- Active Amp-hours
- Minimum battery power required
- Total standby battery power required
- Battery derating factor

If you have more than one control panel in your project, use the *Control panel address* drop-down menu to select the control panel and the battery information for that control panel will populate the window. The *System device*s field outlines all power source devices contained in the selected control panel. Select a device on this tree and all devices drawing power from the selected device are outlined in the *Ancillary devices* field.

The *Power sources* field includes the following information for all power source devices:

- Description
- Hours in standby
- Minutes in alarm
- Seconds in alarm

The *Power sink objects* field lists the following information for all devices drawing power:

- Description
- Duty cycle
- Standby current (mA)
- Alarm current (mA)
- Active current (mA)

All fields in the *Battery calculation* tab are read-only. Use this tab to check the results of the battery calculation and to determine if any devices need to be redistributed. To make any needed changes, you must go *System bus layout tab* on page 44 and change the information programmed there.

Use the *As-built tool* on page 81 to get a printed document of battery calculations for each power source device in your project. This document will show the details for the power source device, all devices drawing power from that power source, and the calculations made to generate the final battery requirement value.

If a power source device does not have any devices drawing power from it, the device will not have a document page in the As-built report.

Cable calculation tab

Use the *Cable calculation* tab to produce the cable length requirements for selected cable types. The calculation results are used in the As-built report.

Use the *Graph setup* and *Wire setup* tabs to set the parameters for the calculation.

Graph setup tab

Use the *Graph setup* tab to set the X and Y axis range for the graph. To return to the default settings, click **Reset**.

Wire setup tab

Use the *Wire setup* tab to set the following parameters:

- Power supply (volts)
- Minimum voltage
- Wire DC resistance (ohms/km
- Added wires to reduce resistance
- Number of power supply wires

Calculate cable length

To calculate cable length, do the following:

1. Set the graph parameters in the *Graph setup* tab.
2. Set the wire parameters in the *Wire setup* tab.
3. Select the wire type in the *Selected wiring* field.
4. Click **Update graph**.

Print cable calculation

To print the results of the cable calculation, you must use the *As-built tool* on page 81.

Chapter 3 Alliance Builder tools

The top row of tools in the tool bar are used for programming functions that are not downloaded to the control panel.

In this chapter:

Device polling tool

The control panel uses polling to communicate with all DGP and RAS devices and gather status information. If a DGP or RAS device is not polled, alarms on any zones associated with the device are not reported or logged.

Use the *Device polling* tool to indicate if you want the control panel to poll devices. We recommend you select **Enable all polling** to ensure that all devices on the system are programmed to be polled by the control panel. This tool can save you a lot of time by enabling polling for all devices and eliminating the need to program each device to be polled.

Select **Disable all polling** if you want to wait until you complete your programming before you enable polling or if you want to only enable polling for specific devices.

Enclosures tool

Use the *Enclosures* tool to open or close all device enclosures on the *System bus layout* tab.

As-built tool

The *As-built* tool (Figure) gathers information from different locations in Alliance Builder and creates a dated report of your project. This report can be saved as a PDF file and printed. Any or all of the following components can be selected for the report:

Project summary. High-level executive summary that includes customer information and tables that list project properties such as zones and doors. You can choose to have the information presented in a single properties table or in multiple tables for each category of information.

CSI specifications. Summary of Alliance specifications that are constant for all Alliance systems. This summary is approximately 30 pages in length.

Brochure. Add an Alliance brochure to the report.

System overview diagram. Details possible Alliance configurations, but is not tied to the devices selected in the project.

Installer wiring info. Choose if you want to add a breakaway relay wiring diagram and/or a telephone wiring diagram to the report.

Bus layouts. Provides a graphic representation for the system and local bus layouts as shown in the *System bus layout* tab and the *Local bus layout* tabs.

Device manuals/datasheets. Provides datasheets for each device type used in the system. Select the options you want. When you add these options it can significantly increase the size of the As-built report.

Point ID address summary. Provides a table with the addresses for all point ID devices in the project.

Wireless serial number summary. Provides a table with the serial number for all wireless devices in the project.

Video integration summary. Provides tables of all TCP/IP video equipment, such as DVMRs and cameras as shown in the *DVMRs/cameras* tool.

Parts list. Lists all parts for the project shown in the *Parts list* tab. You can choose to have the parts separated into two tables, Alliance parts and third party parts, or you can choose to have them combined into a single parts table.

Battery calculations. Battery requirement calculations as for your project devices.

Cable calculations. Cable length requirements as calculated in the *Cable calculation* tab

Wiring diagrams. Wiring diagrams for all devices in the system as shown in the *Wiring diagrams* tab. You can choose to have the diagrams print in high or low resolution. Selecting high resolution can greatly affect the quality of the print, but will also greatly increase the size of the print file. You can also choose to include a door, relay, and zone index.

Page setup options

You can choose what type of branding you want the As-built report to show. If you select **Use standard GE Security name/logo**, the report will print with the GE name and logo on every page. If you want to have a different company name and logo on the report, select **Use dealer company name/logo (if defined)**. The logo must be defined in the Installer administration tool and must have a white background. It cannot be a transparency.

Save the report as a PDF file

We recommend you save the report as a PDF file and print the report from the PDF file. To save the report as a PDF file, do the following:

1. Select all of the required components from the list by selecting them individually or by clicking **Check all**.
2. Click **Save to PDF.**
3. When the dialog box appears, indicate where you want to store the file and click **Save**. The progress bar at the bottom right corner of the window will indicate when the process is complete. You can then print the PDF.
4. Click **Close** to exit the tool.

Print the report

For the best print job, we recommend that you print from a PDF file, as detailed in the section above. But, if you want to print directly from the report, do the following:

1. Select all of the required components from the list.
2. Click **Print**.
3. Click **Close** to exit the tool.

Print preview

To see what the printed report will look like and how long it will be, click **Print preview**. The *Print preview* window shows how each page will print and indicates the number of pages the report will take. You can use the icons provided to view different page layouts and zoom in and out to view page details.

Architecture view tool

Use the *Architecture view* tool to get an overview of how project devices relate to the system and local buses. The device tree in this tool contains all devices in the system layout graphic and indicates the devices supported by each DGP and control panel. The tree indicates the relationships and ties between the devices as well as how the devices are organized in the enclosures.

This tool is a read-only feature. If you want to add, edit, or remove devices, you must make the changes in the *System bus layout* tab.

Auto layout tool

As you add and remove devices in the *System bus layout* tab, the graphic can develop gaps and awkward spacing between elements. Use the *Auto layout* tool to pull the graphic together, eliminating and adjusting space between elements to ensure a clean and compact graphic

Installer administration tool

Use the *Installer administration* tool to add dealer setup information and to add, edit, and remove both installers and installer types.

Dealer setup tab

Use the *Dealer setup* tab to add general information about the dealer that employs this installer. The information entered here is typically used whenever forms are printed through Alliance Builder. Fill in all applicable fields. If a company logo is required to print on the forms, use the browse button to locate the logo and import it into Alliance Builder. The logo needs to have a white background. A transparency cannot be used. Click **Clear logo** to remove the imported logo and default to the GE Security logo.

Installers tab

Select the *Installers* tab to add, edit, or remove installers. The tab provides a list of all existing installers with the following details:

Login name. The *login name* can be a unique company code or ID number and is limited to 16 characters entered as uppercase letters.

Description. The installer type in the description box dictates the functionality and permissions for the installer.

Project directory. The default directory indicates where project files will be stored for this installer.

Add installers

To add installers to the list, do the following:

1. Click **Add**.
2. When the *New/edit installer* window appears, fill in the installer name (a unique login name or code), first and last name (the installer's real name), phone number, mobile phone number, email address, password, and confirm password. Select the installer type from the drop-down list.

3. If the installer type selected permits the installer to create projects, indicate in the project directory where the project files for this installer should be stored.
4. Click **OK**.
5. The installer will be added to the installers list.
6. Click **Close** to exit the tool.

Edit installers

Although you can edit information for all installers, you can only edit the password or directory information for *Alliance Installer.* All other information for *Alliance Installer* cannot be changed.

To edit an existing installer's information, do the following:

1. Select an installer name from the list.
2. Click **Edit**.
3. Change the existing information in the *New/edit installer* window.
4. Click **OK**.
5. The new information will show in the installers list.
6. Click **Close** to exit the tool.

Remove installers

All installers can be removed from the system except *Alliance Installer.* This ensures that the system always has a default installer. Before removing an installer you must use the *Project management* tab to reassign any projects for that installer. Alliance Builder will not allow you to remove an installer that has assigned projects, but will provide a warning notice to alert you to the situation.

To remove an existing installer, do the following:

1. Select an installer name from the list.
2. Click **Remove**.
3. When the confirmation box appears, reconfirm the removal.
4. Click **Close** to exit the tool.

Installer types tab

Select the *Installer types* tab to add, edit or remove installer types. The tab provides a list of all existing installer types.

Add installer types

To add installer types, do the following:

1. Click **Add**.
2. Enter the name for the new installer type. The name must be in 5 to 16 alphanumeric characters long.
3. Select the permissions and functions you want to give this installer type.
4. Click **OK.** The new installer type will be added to the installer type list and be available for selection when new installers are added.
5. Click **Close** to exit the tool.

Edit installer types

You cannot change or edit the *Alliance Installer* type. The permissions and functions for this installer type are set by Alliance Builder.

If you edit an installer type that has already been assigned to active installers, those installers will be affected by the changes to the installer type the next time they use Alliance Builder.

To change information for an existing installer type, do the following:

1. Select the installer type from the installer types list.
2. Click **Edit**.
3. Change the existing information for the installer type.
4. Click **OK**.
5. Click **Close** to exit the tool.

Remove installer types

The *Alliance Installer* type cannot be removed. This ensures that the system always has a default installer type.

You cannot remove an installer type that has been associated with installers. The installers must be removed or their installer type changed before the installer type can be removed. If you attempt to remove an associated installer type, Alliance Builder will provide a warning notice to alert you to the situation.

To remove an existing installer type, do the following:

1. Select an installer type from the list.
2. Click **Remove**.
3. When the confirmation box appears, reconfirm the removal.
4. Click **Close** to exit the tool.

Project management tab

Use the *Project management* tab to manage all projects that your permissions include. To delete a project, select the project on the list and click **Delete selected projects**. To reassign projects, select the project from the list and click **Reassign selected projects**. It is important to always reassign projects before removing the installers assigned to the projects. The project list on the *Project management* tab is a reflection of the project list on the Project list tab and is provided in this tool to make programming user information faster and easier.

Device property window tool

The *Device property window* tool invokes the property window. This window enables you to program the selected property while easily accessing related information in other areas of Alliance Builder. This can save you a lot of time when you are programming two related features and need to be able to see and program them at the same time.

If you have the property window open in a programming area and you change related properties in the main interface, the information in the property window will not show the changes. When you click on the property window it will show the updated information.

When you have finished programming the item, click **Close** to exit the tool. All programming done in the property window will be saved and reflected in your project.

See *Property programming* on page 18 for details on various methods of changing property programming.

Export tool

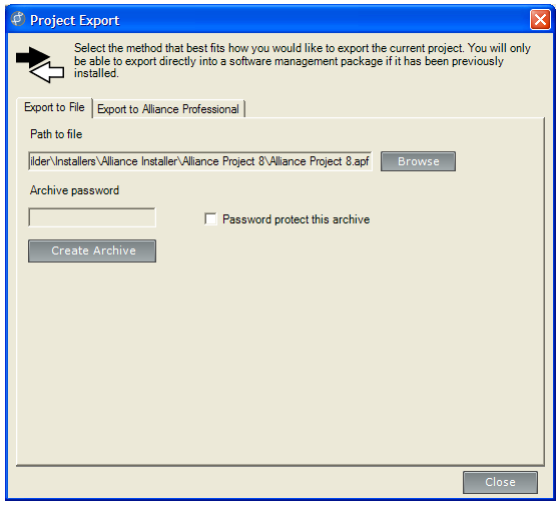
Use the *Export* tool to export a project to an archive file or to software management systems.

Select your software management system from the drop-down menu. If a software management system is not supported by Alliance Builder it will be inactive (grayed out).

To export a project to an archive file, do the following:

1. Select the *Export to file* tab (*Figure 24*).

Figure 24. Export to file

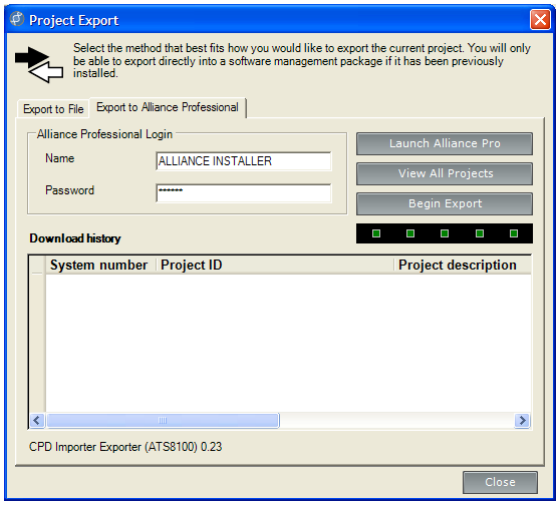


2. Use the *Browse* button to designate the location for the file.
3. If you want password protection, select **Password protect this archive** and type a password in the box.
4. Click **Create archive**.

To export a project to Alliance Professional, do the following:

1. Select the *Export to Alliance Professional* tab (*Figure 25*).

Figure 25. Export to Alliance Professional



2. Alliance Professional must be loaded on your computer. If you have not launched Alliance Professional since loading the program, type in your name and password and click **Launch Alliance Professional**. Launching the program creates a database that is necessary for the export function.
3. Click **Begin export**.
4. Click **Close** to exit the tool.

If you want to view a list of projects that have been exported to Alliance Professional, click **View all projects**. The exported projects will appear in the Download history field and will include the following information for each project:

- System number
- Project ID
- Project description
- Download (export) date

Chapter 4 Panel/device tools

The bottom two rows of tools in the tool bar are used for programming that will be downloaded to the control panel.

In this chapter:

Device addressing tool

The *Device addressing* tool allows you to view the device addresses for your project.

Software managed mode

The software manages the addressing and makes programming the project easier, ensuring that the device addresses are always correct. Devices will be automatically addressed as they are added to the project and updated as changes are made.

If a project is imported, the addresses already set in the project will change to follow the software addressing rules.

Manually managed mode (not available at this time)

Device address configuration

The *Device address configuration* window lists all device addresses assigned to DGP and RAS system devices. The information is a read-only feature. The following information is provided for all devices on the DGP and RAS tabs:

Part number. The Alliance part number for the device

Description. The description supplied by Alliance Builder

Address number. The address number for the device in the project

Programming viewers tool

Use this tool to quickly display properties programmed in your project. Although not all programmed properties are listed, the basic properties for each category are shown.

The *Programming viewer* tool is a read-only feature and cannot be used to edit the information shown.

RAS devices viewer

This viewer shows the following basic RAS device properties programmed in the project:

Address. System address number (1 to 16) assigned by Alliance Builder

Description. RAS description

Alarm group. Alarm group (1 to 138) assigned to the RAS

Door event flag. Event flag (0 to 255) assigned to the RAS

Is polled. If checked, the RAS is programmed to be polled.

LCD RAS. If checked, the RAS has an LCD keypad.

Use entry/exit buzzer. If checked, the RAS buzzer will sound when associated entry/exit timers start.

The properties shown in the viewer are programmed in the *System bus layout* tab. For information on all RAS programming options, see *RAS (remote arming stations)* on page 112.

DGP devices viewer

This viewer shows the following basic DGP device properties programmed in the project:

Address. System address number (1 to 15) assigned by Alliance Builder

Description. DGP description

Is polled. If checked, the DGP is programmed to be polled.

DGP type. DGP type (standard, 4-door controller, wireless, or point ID) indicated by the DGP part number

The properties shown in the viewer are programmed in the *System bus layout* tab. For information on all DGP programming options, see *DGP (data gathering panels)* on page 120, *4-door/elevator controllers* on page 123, *Point ID DGP* on page 129, and *Wireless DGP* on page 132.

Zones viewer

This tab shows the following basic zone properties programmed in the project:

Number. Zone number.

Name. Descriptive zone name that will be transferred to the control panel and RAS.

Zone type. Zone type (0 to 70) that specifies the behavior associated with the zone.

Zone reporting code. The reporting code is a reflection of the zone type that is sent to the central station.

Assigned areas. Areas assigned to the zone.

The properties shown in the viewer are programmed in the *Control panel programming* tab. For information on all zone programming options, see *Zones* on page 236.

Relays viewer

This tab shows the following basic relay properties programmed in the project:

Number. Relay number.

Type. Physical or virtual.

Description. Relay description.

Event flag. Event flag that will activate the relay.

Time zone. Time zone (0 to 64) when the relay can be active or inactive

The properties shown in the viewer are programmed in the *Control panel programming* tab. For information on all relay programming options, see *Relays* on page 230.

Relay control groups viewer

This tab shows information for all relay control groups currently defined for your project. The list will show if there are any duplicate relay control groups assigned to more than one RAS device.

RAS address. The address of the RAS associated with the relay control group.

Description. Relay control group description.

Relay number. The relay number of the first relay of the relay control group.

Event flag. The event flag activated for the relay.

Click on a sub item to see the RAS devices programmed for that relay.

To remove a relay control group, select the line on the list and use your delete key. This is the only way to remove a relay control group without removing the associated RAS device.

For information on relay control group programming, see *RAS (remote arming stations)* on page 112.

Doors viewer

This tab shows the number and description of all doors programmed to be supported by the control panel. This includes up to 16 RAS devices on the system bus, as well as up to 48 intelligent doors on 4-door controller local buses.

Number. Door number which is either a RAS address or just a Door number.

Description. Door description used for programming purposes, not downloaded to the control panel

Type. The type is a combination of:

- Device type (card reader or keypad)
- Door type (RAS or intelligent door)

To find a particular door on the list, type in the door name or number in the appropriate search box and click **Search**.

The status bar at the bottom of the viewer indicates the minimum, maximum, and number of doors used.

The properties shown in the viewer are programmed in the *Local bus layout* tab. For information on all door programming options, see *Doors* on page 138.

Alarm groups viewer

This tab shows the following basic alarm group properties programmed for the project:

Number. Alarm group number.

Name. Descriptive alarm group name that will be transferred to the control panel and the RAS device.

Description. Alarm group description.

Areas. Areas where the alarm group will have alarm control.

Time zone. The time zone assigned to the alarm group defines when the alarm group is active.

Is user alarm group. If checked, the alarm group is assigned to users. If not checked, the alarm group is assigned to RAS/Door devices.

The properties shown in the viewer are programmed in the *Control panel programming* tab. For information on all alarm group programming options see *Alarm groups* on page 188.

Areas viewer

This tab shows the following basic area properties programmed in the project:

Number. Area number.

Name. Descriptive area name that will be transferred to the control panel and RAS

Entry time. Amount of time programmed for the entry timer

Exit time. Amount of time programmed for the exit timer

Armed event flag. The event flag activated when the area is armed

Disarmed event flag. The event flag activated when the area is disarmed

The properties shown in the viewer are programmed in the *Control panel programming* tab. For information on all area programming options, see *Areas* on page 178.

Time zones viewer

This tab shows the following information for all time zones programmed for the project:

Number. Time zone number

Description. Time zone description

Type. Hard or soft time zone

The properties shown in the viewer are programmed in the *Control panel programming* tab. For information on all time zone programming options, see *Hard time zones* on page 226 and *Soft time zones* on page 233.

Wireless serial numbers viewer

This tab shows the following information for wireless devices currently used in your project:

Type. The type of wireless device

Part number. The part number used to order the device

Description. A programming description for the device.

DGP address. The DGP system address number for the wireless DGP that controls the device.

Serial number. Each wireless device added to the project requires a unique serial number that is typically listed on the outside of its shipping box.

The properties shown in the viewer are programmed in the *System bus layout* tab. For information on all wireless device programming options, see *Wireless DGP* on page 132.

Arm/disarm viewer

This tab shows all zones and alarm groups assigned to a selected area programmed for the project.

When an area is selected in the *Area* field, the area's related zone and alarm group information will display. This indicates the zones and areas that users in a specific alarm group can arm and disarm.

The properties shown in the viewer are programmed in the *Control panel programming* tab.

Text words tool

Use the *Text words* tool to view the text word library (see *Text word library* on page 308). The library contains up to 900 predefined text words and up to 100 user-defined text words. The library includes a number and description for each text word. A text word can be a single word or a short phrase, such as *Area Ten*, with a maximum of 16 characters.

Text words are downloaded to the control panel and are used to display words and phrases in LCD keypads, reports, and software management programs.

To find specific text words, scroll through the list or enter the text word or a text word number in the appropriate search box and click **Search.**

To add user-defined words to the library, use the *Control panel programming* tab.

Event flag descriptions tool

Event flags are one of the most important aspects of the Alliance system. Event flags are used by the system in order to signal an event. When a certain event occurs event flags are raised to notify other programming options to perform specified functions. Use this tool to view the event flags for your project.

The event flag descriptions are not downloaded to the control panel, but are used to make programming the system easier. It is very important to document event flag descriptions. These descriptions help to eliminate mistakes and confusion when you need to make changes in the future.

There are two types of event flags, predefined and custom. Predefined event flags, **numbered from 1 to 16, can not be changed or removed** (see *Predefined event flags* on page 265)**.** Custom event flags can be added, edited, or removed from the list by changing the programming in the Panel programming tab.

The list includes the following information:

Number. Event flag number (1 to 255)

Description. A brief description that indicates to the installer the purpose of the event flag for programming options.

To search the list for a particular event flag, type in the event flag name or number in the appropriate search box and click **Search**.

To see how many event flag descriptions have been programmed, see the minimum, maximum, and amount used in the status bar at the bottom of the tool.

Timers tool

Use the *Timers* tool to program timers for the system.

Select the tab for the type of timer you want to program, then use the up/down buttons to set the time for each timer needed. You can enter a value instead of using the up/down buttons, but if the value entered is outside the accepted range, it will default to the maximum value within the range. We recommend you always use the up/down arrows to avoid programming errors.

Timers are accurate to +/- 1 of the value entered, therefore avoid programming values of 1 second or 1 minute. If a timer is set to 0, it will not be used.

To get a brief description of each timer, select a tab and mouse over the timer option.

Alarm group restriction timers

Alarm group restriction timers determine the amount of time the associated areas will be disarmed. After the specified amount of time has elapsed, the area will automatically rearm. If the time is left at zero for an alarm group restriction timer, the associated area will not automatically rearm.

To set alarm group restriction timers, do the following:

1. Use the up/down buttons to set the time (in minutes) for each alarm group restriction needed (1 to 7).
2. Click **Close** to exit the tool.

Alarm control timers

The following alarm control timers are provided:

Warning time. The time a warning will sound indicating the areas are about to arm.(Alarm group restrictions must be used and areas must be programmed for timed disarmed)

Delay reporting alarms time. The delay time before a burglar alarm (BA) or BA class tamper alarm (TA) is reported to the central station. It can be used to prevent alarm reporting for users that have problems disarming their area in time.

Double-knock interval. The maximum permitted time between a zone becoming active for first time becoming active for the second time. If this time is exceeded, an alarm condition is registered. This timer is used in conjunction with the double-knock duration timer.

Delayed disarm alarm time. The delay time before an alarm from a delayed disarmed alarm is reported to the central station.

Local alarm reminder. The time that can elapse between acknowledging a local alarm and an alarm reoccurring, including the audible alert.

Double-knock duration. The maximum permitted time a zone may remain active. If the time is exceeded, an alarm condition is registered. This timer is used in conjunction with the double-knock interval timer.

To set alarm control timers, do the following:

1. Use the up/down buttons to set the time for any required control timers.
2. Click **Close** to exit the tool.

Diagnostic timers

The following diagnostic timers are provided:

Zone test time. The maximum time required to perform a test on an individual zone.

Technician service time. The time a technician, with service technician privileges, has to service the system.

Disarm test time. The time available to do a disarm test.

Event flag test time. The time the testing event flag is triggered to activate devices in order to perform an arm test. The event flag will only be triggered for half the programmed time. The remaining time is used to allow the device to switch back to the normal state.

AC fail time. The delay time before an AC fail is reported to the central station.

Arm test time. The time available to do a arm test.

To set diagnostic timers, do the following:

1. Use the up/down buttons to set the time for any required diagnostic timers.
2. Click **Close** to exit the tool.

RAS access timers

The following RAS access timers are provided:

RAS unlock time. The time a door's RAS device will be unlocked when the door's corresponding event flag has been triggered. This time applies to all system doors.

Screensaver timeout. The time it takes for the RAS screensaver to time out. The screensaver timer will be reset with the programmed time every time a RAS key is pressed when the screensaver is active.

RAS card + PIN timeout. If a user is required to enter a PIN and badge a card in order to gain access, this is the maximum time allowed between the two actions. If the time elapses, the user must repeat the process until the user is locked out.

To set the access timers, do the following:

1. Use the up/down buttons to set the time for any required access timers.
2. Click **Close** to exit the tool.

Siren timers

The following siren timers are provided:

External siren time. The time for the on-board external siren drivers to activate.

External siren delay time. The time that elapses before the external siren cuts-off after activation.

Internal siren time. The time for the on-board internal siren drivers to activate.

Internal siren delay time. The time that elapses before the internal siren cuts-off after activation.

To set siren timers, do the following:

1. Use the up/down buttons to set the time for any required siren timers.
2. Click **Close** to exit the tool.

Programming validator tool

Use the *Programming validator* tool to search the project for problems with programming options. The *Programming validator* window provides a list of errors found in the system with the error type, programming category, property, property type, and number in error.

This tool is only used to indicate the errors found. To correct the errors, you must go back to the programming category indicated to change the programming and resolve the problem. Select an error row in the list and use the **Click to invoke property for the selected row** link. The property window will open containing the programming related to the error. Correct the programming error and click **Close** to exit the window.

Virtual relays tool

Use the *Virtual relays* tool to create relays that do not exist in hardware, but can be used for general programming.

To add virtual relays, do the following:

1. Right-click on the folder and select **Add virtual relay**.
2. In the number assignment window, select a number from the list for the relay and click **OK** or double-click the number to make the assignment.
3. Use the *Relay programming* field to program the relay. Give the relay a description, indicate if it is inverted, and specify the parameters that determine how this relay will be activated.
4. Click **Close** to exit the tool.

To remove virtual relays from the list, do the following:

1. Right-click on the relay on the list and select **Remove virtual relay**.
2. Click **Close** to exit the tool.

For additional information on relays, see *Relays* on page 230. For information on programming physical relays, see *Control panel programming tab* on page 62.

DVMRs/camera tool

Use the read-only *DVMRs/cameras* tool to view DVMRs and cameras defined in your project. Use the drop-down menu to select how you want to view the list. If you select **DVMR/cameras**, you will get a list that includes the item, description, DVMR number, camera number, and preset number.

You must use the *System bus layout* tab to add DVMRs to the system and program the cameras (see *Add cameras to a DVMR* on page 56).

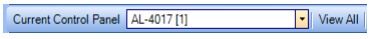
Current control panel tool

The *Current control panel* tool (*Figure 26*) includes the following options:

Control panel. Select the control panel you want to program from the drop-down list.

View all. View a list of all control panels for the current project along with related device totals for each control panel.

Figure 26. Current control panel tool



Since Alliance systems can have up to seven individually programmed control panels, it is very important to always know which control panel is currently selected. In systems with only one control panel, this will not be an issue. Alliance will automatically name the first control panel you add to the system Control Panel (1). That control panel will remain selected until another control panel is added to the system.

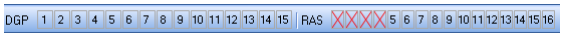
For systems with multiple control panels, the information shown in the menus, toolbar, tabs, and status bar will reflect only the information for the control panel indicated in the current control panel field.

To add or remove control panels from the project, see *Control panel tab* on page 46.

DGP/RAS numbering graphics

Use the DGP/RAS numbering graphics (*Figure 27*) to quickly see the number of DGP and RAS devices that have been used in your project and the number of devices you can add to your project. Alliance builder will keep track of the devices and update the graphics as devices are added or deleted from your project. For information on how numbering is applied to Alliance projects, see *Numbering* on page 324.

Figure 27. DGP/RAS numbering graphics



Chapter 5 RAS programming features

This chapter provides an overview of remote arming station (RAS) devices and programming features.

RAS (remote arming stations)

RAS (remote arming stations) are keypads and card readers used to control arming and disarming of areas in system, access control, and system programming (LCD keypads). Keypads and readers can use various input methods to arm and disarm areas such as user PIN codes, 3x Badging, and PIN + card. A maximum of 16 RAS devices are allowed on the system bus and an additional 16 RAS devices are allowed per local bus/ reader ports. Most keypads and readers can connect directly to the system or a local bus in the system. However, Wiegand readers require an AL-1170 reader interface device.

The ability to arm and disarm areas from the RAS device is governed by both the assigned RAS alarm group and the alarm group assigned to the user. Both alarm groups must have alarm control enabled in order to arm/disarm areas. Once a user either enters their PIN code at a keypad or badges their card at a reader, depending on a combination of RAS/alarm group options, the system will arm/disarm. For example, if a card reader with the *card auto disarm* option enabled and an assigned alarm group allowing alarm control is accessed by a user with equivalent privileges, the system will disarm all areas that match between the two alarm groups.

Although many people consider keypads and card-readers to be doors, the system treats the first 16 devices on the system bus as simply RAS devices. The system only considers RAS devices doors when they are connected to a 4-door controller local bus. The main distinction between the two is the lack of intelligent capability found in the basic RAS device. Basic RAS devices have no built-in provisions for features such as antipassback, request to exit, and door shunting. These are all features found within doors connected to 4-door controllers.

Types

Alliance provides the following types of RAS devices:

Keypads. Keypads arm and disarm areas and allow access through user PIN numbers. Some keypad devices include an LCD display that can show information about the system, such as when a zone is in alarm, and also allow an installer to program the system.

Readers. Readers arm and disarm areas and allow access through user cards. The system supports Smart Card readers as well as mag swipe readers.

Interface modules. Interface modules support the ability to add Wiegand readers to the RS485 bus. Applicable to both the system and the local bus.

Functions

RAS devices can be used for the following functions:

Arm/disarm. RAS devices can be used to arm or disarm areas by a privileged user.

System programming. LCD keypads allow a privileged user to make programming changes to the security system via the keypad interface.

User programming. If a user with sufficient privilege accesses an LCD keypad, a user can be added or edited directly from the keypad.

Monitoring. Area alarms and access can be monitored using an LCD keypad.

Open door. RAS devices can provide access capability. Typical uses include entering a PIN code on a keypad or badging a card reader in order to open a door.

Programming

The following programming options are available for RAS devices:

RAS number

Range: 1 to 16

Specify which RAS is being programmed (same as the system bus address). The first RAS device address on the system bus must be an LCD keypad. The DIP switch setting applied to the device will be one less then the assigned address. For example, RAS address 1 would require setting the DIP switches to zero (1 – 1 = 0).

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Area alarm group

Range: 1 to 138

The area alarm group assigned to a RAS device determines which areas can be armed and disarmed by the device.

Door event flag

Range: 0 to 255

The door event flag is raised when the RAS device grants access to a user. This event flag is typically used by a number of other programming features within the system, such as macro programming. The *unlock time* option in *Timers programming* (see *RAS unlock time* on page 174) determines how long the door will remain open.

Menu alarm group

Range: 1 to 138

The menu alarm group assigned to a RAS device determines which features can be accessed via the keypad, such as the installation menu, system status, history, and device control. In order for a user to access certain menu options, the user must have the same menu permissions enabled (through the alarm group assigned to the user) as the RAS device.

Relay (output) control group

Range: 0 to 32

Purpose: Specify the relay control group connected to the RAS device. When a relay control group is assigned to a RAS device, the open collector relay (OUT) terminal follows the first relay of the relay control group. See *Numbering* on page 324. *Table 5* shows relay groups and their related relay numbers.

Table 5. Relay numbering

Group	Relay number		Group	Relay number
1	1		17	129
2	9		18	137
3	17		19	145
4	25		20	153
5	33		21	161
6	41		22	169
7	49		23	177
8	57		24	185
9	65		25	193
10	73		26	201
11	81		27	209
12	89		28	217
13	97		29	225
14	105		30	233
15	113		31	241
16	121		32	249

RAS options

Poll RAS	**Enabled**: The control panel will continuously poll the RAS device. **Disabled:** The control panel will not poll the RAS device.
LCD keypad	**Enabled:** The RAS device has an LCD display. **Disabled:** The RAS device does not have an LCD display.
Toggle area status	**Enabled:** Provides the ability to toggle area status via the keypad. The user PIN is entered, followed by **ON**, **OFF**, or **ENTER**. If a list appears, pressing the area number and then **ENTER** will toggle the area status. Enabling this option will cause the **ON** and **OFF** keys to lose their default functionality. **Disabled:** Normal alarm control functionality. This option assumes the RAS device is an LCD keypad. Do not use this option if the *ENTER key opens door only* option is enabled.
ENTER key opens door only	**Enabled:** The **ENTER** key can be used to open a door. **Disabled:** The **ENTER** key opens a door and provides alarm/reset control. This option saves the user from having to click the **ON/OFF** keys when performing alarm control. It is highly recommended that this option be enabled for the best possible LCD keypad user interface.
Alarm codes opens door	**Enabled:** When a user either badges their card or enters a PIN, and has alarm control (via alarm group and door group), the door will open. For example, when enabled, this option causes the door event flag to be raised, which in turn, opens the door. **Disabled:** Under the same scenario, the door will not open.
Display shunted zones on RAS	**Enabled:** When a zone is shunted, *Zone shunted* will appear on the display. **Disabled:** Nothing is displayed when the zone is shunted. This option assumes the RAS device is an LCD keypad.
Arm/disarm using one key	**Enabled:** Allows the user to arm or disarm an area by entering their user code and the area number without having to press **ENTER** on the keypad after selecting the area. **Disabled:** The user will need to press **ENTER** on the keypad after entering their user code to arm or disarm an area.

Card auto disarm	**Enabled:** Badging cards disarms areas without using the **OFF** key. **Disabled:** Badging cards does not disarm areas. Areas are disarmed manually. This option assumes the RAS device is a card reader.
Disable status LEDs	**Enabled:** The card reader LEDs will be displayed when the control panel polls the RAS device. **Disabled:** Normal card reader LED function. This option assumes the RAS device is a card reader. Certain door reader settings override this function. It may be necessary to alter the *LED* option in *Door reader programming* (see *LED* on page 151).
Card always arms/disarms	**Enabled:** Badging a card reader allows arming/disarming areas without using the **ON**/**OFF** keys. **Disabled:** Normal alarm control. This option assumes the RAS device is a card reader. The card's user alarm group and the RAS device's (card reader's) alarm group must both allow arm/disarm functions in order for this function to work.
Reset without code	**Enabled:** Allows users to reset alarms by pressing **ENTER**, **ENTER**, **0**, **ENTER** on the keypad. The areas in alarm have to be assigned to the RAS alarm group. **Disabled:** Reset can only occur by entering the user PIN code and navigating through the menu on the keypad. This option assumes the RAS device is an LCD keypad.
Restrict alarm group restriction to disarm	**Enabled:** Users with alarm group restrictions can only disarm or delay automatic arming. It cannot be used for alarm group restrictions with arm and reset. **Disabled:** There is no restriction.
Use entry/exit buzzer	**Enabled:** The RAS device buzzer sounds when the entry/exit timers associated with the area assigned to the RAS device start. **Disabled:** The RAS buzzer will not sound when the entry/exit timers start. The entry time must be over 10 seconds.
Timed lockout on wrong codes	**Enabled:** When an invalid code (defined as five consecutive invalid entries) is entered, the RAS device will lockout for 90 seconds. **Disabled:** The RAS device is available after an invalid code is entered.

Card arms after 3 badges	**Enabled:** Allow the user to arm the assigned areas by badging their card three consecutive times within a ten second window. **Disabled:** Three times badging functionality is disabled. This option assumes the RAS device is a card reader.

Chapter 6 DGP programming features

This chapter provides an overview of data gathering panels (DGP) devices and programming features.

In this chapter:

DGP (data gathering panels)

DGP (data gathering panels), depending on the device type, can provide expansion capabilities, redundant databases, access control, zone monitoring, and many other features. DGP devices connect to the control panel through the RS485 system bus. During system operation, the control panel will continuously poll the DGP in order to obtain status information.

There are a maximum of 15 DGP devices allowed per control panel (for 4-door/elevator controllers, the maximum number is 12). By default, each DGP device consumes a single DGP address. Typically, DIP switches are used to assign the address on the device itself. However, by expanding a DGP device with zone and relay expansion devices, a DGP can consume two addresses. Under this scenario, other devices within the system cannot use the second address (see *Numbering* on page 324).

Types

Alliance provides the following types of DGP devices:

Standard DGP. Supports standard DGP options, such as zone/relay expansion.

4-door controller DGP. The 4-door controller DGP is a specialized device for providing intelligent door control in the system. Each 4-door controller can control four doors, each with two IN-readers and two OUT-readers. The 4-door controller is intelligent in that it contains a sub-set of the control panel database with all of the user's access rights for the doors it controls. If the control panel should stop functioning for any reason, the 4-door controller would continue to provide access and logging. The 4-door controller does not provide any zone expansion capabilities. See *4-door/elevator controllers* on page 123.

4-elevator controller DGP. The 4-elevator controller DGP is similar to the 4-door controller, with the addition of elevator control for the system. See *4-door/elevator controllers* on page 123

Wireless DGP. A wireless DGP is similar to a standard DGP, except the devices controlled by the DGP are wireless devices. See *Wireless DGP* on page 132.

Point ID DGP. A point ID DGP is similar to a standard DGP, except the devices controlled by the DGP are addressed. See *Point ID DGP* on page 129.

Functions

DGP devices can be used for the following functions:

Polled by control panel. The control panel will communicate with the DGP device over the system bus in order to gather status information.

Siren. Some DGP devices are equipped with their own siren which will sound when one of the zones goes into alarm

Zone/relay expansion. Most DGP devices can support up to 32 zones through expansion (some DGPs, such as the 4-door controller do not support zone expansion). Relay expansion is typically limited to 16 relays (two 8-way relay expansion boards)

Redundant databases. Some DGP devices, such as the 4-door controller, maintain an independent database from the control panel. If the system bus is severed, the device does not have to communicate with the control panel in order to grant access to a user.

Bus address. A DGP is assigned a bus address that, in turn, determines the zone/relay numbering.

Localized wiring. DGP devices provide the capability to install zones, relays and power to a location that is a substantial distance from the control panel. This allows fewer wires to be run and localized power and battery backup to be used.

Doors/floors. Some DGP devices provide additional intelligent functionality, such as the 4-door and 4-elevator controllers.

Programming

The following programming options are available for DGP devices:

DGP number

Range: 1 to 15 (for a 4-door/elevator controller DGP, the range is 1 to 12)

Specify which DGP is being programmed (the system bus address).

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Poll DGP

Determine if the control panel should poll this DGP device. If a DGP is not polled, alarms on any zones associated with the DGP are not reported or logged.

DGP type

Specify the type of DGP you are programming (see *Types* on page 120). The options include:

- Standard DGP
- 4-Door Controller DGP
- 4-Elevator Controller DGP
- Wireless DGP
- Point ID DGP

4-door/elevator controllers

The 4-door controller provides intelligent door control for the system, including RTE (request to exit), antipassback, region support, DOTL (door open too long), and various access capabilities. The 4-elevator controller is similar to the 4-door controller with the addition of elevator control. A maximum of twelve 4-door/elevator controllers are allowed per control panel.

Although they are similar to the control panel, the 4-door/elevator controllers are programmed as DGPs (data gathering panels). As such, the system requires that you add the controllers as a DGP in *DGP programming* before you program the 4-door/elevator controller programming options.

The four reader ports located on the controller are, by default, the IN readers for the door. Each of these four doors has one reader port assigned. The reader ports have the following assignments:

- Reader Port 1: Assigned bus address 1 (RAS 1)
- Reader Port 2: Assigned bus address 2 (RAS 2)
- Reader Port 3: Assigned bus address 3 (RAS 3)
- Reader Port 4: Assigned bus address 4 (RAS 4)

Some devices, such as the Wiegand reader, do not have provisions for bus addresses. Therefore, when configuring RAS devices within the controller, the first four RAS numbers correspond to the reader ports. The reader port number follows the RAS number/address.

Door RAS numbering

Table 6 shows the door RAS numbering scheme.

Table 6. Door RAS numbering

Door number	IN RAS address	IN RAS address	OUT RAS address	OUT RAS address
Door 1	1 (reader port 1)	5	9	13
Door 2	2 (reader port 2)	6	10	14
Door 3	3 (reader port 3)	7	11	15
Door 4	4 (reader port 4)	8	12	16

Functions

The 4-door/elevator controller DGP devices can be used for the following functions:

Unique DGP programming. Provides programming that goes outside the bounds of the DGP programming section

Output controllers. Specifies output controllers connected to the door/elevator controller

RAS devices. Configures RAS devices connected to the door/elevator controller's local bus

Timers. Assigns specific times for badging a reader or entering a PIN on a keypad

Events. Configures door/elevator controller specific events

Card batches. Handles card batching

Note: Only applicable to door/elevator controllers without IUM memory modules.

Programming

The following programming options are available for 4-door/elevator controllers:

DGP

Range: 1 to 12

Specify the DGP bus address. This should be the same as the address specified in *DGP programming* for this controller (see *DGP number* on page 122).

Description

Specify a 40-character text description of the DGP. The description is not transferred to the device, and is only used by the management software.

Output controllers

Range: 0 to 32

Specify the number of non-clocked (not driven by a clock on the control panel) output controllers connected to the controller. The controller can only access the first 16 relays,

while the system can access relays that go beyond the first 16. For example, if a controller has four 8-way relay expansion boards attached, the controller can access logical relays 1 to 16, but the rest of the system can access logical relays 17 to 32.

Number of prefix digits

Range: 0 to 4

This value should mirror the *Number of prefix digits* on page 254.

Poll RAS

Specify which local bus RAS devices should be polled by the controller. Refer to *Table 6, Door RAS numbering* on page 123 for more information on how to identify RAS devices on the controller.

LCD RAS fitted

Specify which local bus RAS devices are LCD keypads. Refer to *Table 6, Door RAS numbering* on page 123 for more information on how to identify RAS devices on the controller.

RAS RTE zone

Specify which local bus RAS devices support RTE (request-to-exit) and require the button to be wired to the RTE/IN terminal on the RAS device. Refer to *Table 6, Door RAS numbering* on page 123 for more information on how to identify RAS devices on the controller.

Toggle RAS

Enable/disable local bus RAS toggle mode (only supported by keypad devices).

Enabled: A single key will toggle arming/disarming.

Disabled: Two distinct keys will arm/disarm.

Table 7 shows the keypad input and toggle modes.

Table 7. Keypad inputs and toggle modes

Keypad input	Toggle mode
PIN + **ENTER** or **#**	**Enabled:** Toggles the arm/disarm state **Disabled:** Arms
PIN + **MENU** or *****	**Enabled:** Toggles the arm/disarm state **Disabled:** Disarms

Card to PIN time

If a user is required to enter a PIN and badge a card in order to gain access, this is the maximum time allowed between the two actions. If the time elapses, the user must repeat the process.

Two card time

If two users are required to enter a PIN or badge a card in order to gain access, this is the maximum time allowed between the first user entering a PIN or badging a card and the second user entering a PIN or badging a card. If the time elapses, the users must repeat the process.

Multiple badge time

If a door has been programmed to support the *3x badge* option in *RAS programming* (see *RAS options* on page 116), this is the maximum time allowed between the first badge and the third badge. If the time elapses, the user must repeat the process.

Region count limit

Set a value which, when reached, will cause the region count limit flag to be raised. This event flag can then be used in door macro logic programming.

Elevator programming options

The following options are only used by the 4-elevator controller and do not apply to the 4-door controller.

Starting floor number

Specify the starting floor this 4-elevator controller will control.

Last floor number

Specify the last floor this 4-elevator controller will control.

Starting relay number

Specify the starting physical relay number this 4-elevator controller will use to arm/disarm floors.

Zones monitor floor selected

Specify how zones are used to monitor floors.

Enabled: Zones are used to monitor the selected floor and a report is sent to the printer and management software.

Disabled: Zones are used for alarm monitoring.

Wait for floor selection

Specify how the elevator will wait for floor selection.

Enabled: The elevator will wait for only one floor to be selected before going on.

Disabled: When the user is allowed access to multiple floors, multiple floor may be selected.

Starting zone number

Specify the starting zone number this 4-elevator controller will use to monitor floors.

Elevator override group

Specify a floor group number programmed with floors and a time zone. The elevator override group determines the floors that may be freely accessed in the elevator controls and the times the floors can be disarmed without using a valid card or PIN at the elevator reader.

Security zone number

Specify the zone number that will control the elevator security group. The *zones monitor floor selected* option must be disabled, if the security group zone is used.

Elevator security group

Specify a floor group number. Each floor group is programmed with floors and a time zone. The elevator override group determines the floors that may be freely accessed in the elevator controls and the times that the floors may be accessed provided the security group zone is switched on.

Total floors

Specify the number of floors available for this 4-elevator controller.

Point ID DGP

The point ID DGP controls addressable point ID devices. Although similar to a control panel, the point ID DGP is programmed as a DGP (data gathering panel). As such, the system requires that you add the DGP to the system in *DGP programming*. All other point ID specific programming options are covered in this section.

Once the DGP is added to the system, you can add/configure point ID devices through point ID device programming. Point ID devices have onboard DIP switches used to assign a point ID address. The combination of DGP/point ID address results in a physical zone number (see *Numbering* on page 324) in the Alliance system. In addition, the DGP has a learn mode used to automatically obtain device information without specific programming.

The DGP default polling mode (extended) polls up to 16 devices with reporting information such as *device changed* and *antimask tamper.*

Programming

The following programming options are available for point ID DGP devices:

DGP number

Range: 1 to 15

Specify the DGP address that the DGP will have in the Alliance system. This should be the same as the address specified in *DGP programming* for this controller (see *DGP number* on page 122).

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

DGP address mode

Specify the number of DGP addresses reserved for the DGP that drives the total number of point ID devices allowed for the DGP. The choices are:

1 DGP address. Allows up to 16 zones and 16 relays with 1 address.

1 DGP address plus expansion. Allows up to 32 zones and 16 relays with 2 addresses. Since each DGP address is limited to a maximum of 16 zones, when the number of zones exceeds 16, this mode reserves 2 consecutive DGP addresses.

Point ID devices

The category assigned to the device dictates the programming options available to the device. For some DGP devices the address is the only information that needs to be programmed. Other devices, such as IO devices require additional features to be programmed.

Point ID device categories

All point ID devices are assigned one of the following categories:

- Miscellaneous
- PIR
- Glassbreak
- Conventional smoke
- Analog smoke
- IO

Point ID device zone/relay numbering

When a point ID device is added to a point ID DGP, the device is assigned a system zone number. This number is based on both the DGP system address (see *Numbering* on page 324) and the address assigned to the device using the DIP switches. The zone range is determined by the *DGP address mode* assigned to the DGP. If the mode is set to *1 DGP address*, the maximum number of zones will be 16. If the mode is set to *1 zone address plus expansion*, the maximum number of zones will be 32.

Example 1. The point ID DGP system address is set to 2 and the device is assigned point ID device address 1. Since the DGP 2 zone range is 33 to 48 and the device address is 1, the associated zone number for the device will be 33.

Example 2. The point ID DGP system address is set to 3 and the device is assigned point ID device address 4. Since the DGP 3 zone range is 49 to 64 and the device address is 4, the associated zone number for the device will be 52.

Relay numbering follows the same rules, but to configure relays, the point ID device category must be an IO and the device must have onboard relays.

Example 1. The point ID DGP system address is set to 2 and the device is assigned point ID device address 1. Since the DGP 2 zone range is 33 to 48 and the device address is 1, the associated relay number for the device is 33.

Example 2. The point ID DGP system address is set to 3 and the device is assigned point ID device address 4. Since the DGP 3 zone range is 49 to 64 and the device address is 4, the associated relay number for the device will be 52.

Memory locations

For point ID IO devices nine memory locations are provided for additional programming. Binary values are assigned to the locations to program the following options:

- Output/relay programming
- Zone types
- Output/relay supervision
- EOL value
- Number of inputs/zones and/or number of output/relays

Refer to the installation manual for the point ID DGP for details on programming memory locations.

Wireless DGP

The wireless DGP provides wireless zones and fobs as well as standard DGP functions. Each DGP can support up to 32 zones and up to 16 fob sensors. Zone sensors can be anything from glassbreak detectors to PIR devices, while key fobs are tied to user or relay numbers and provide on/off or arm/disarm facilities such as panic buttons.

Every wireless device is assigned a unique serial number during manufacturing. The serial number can be found on the box label for the device. Once the serial number has been entered into the system, up to four zones will be assigned to the device. Supervision options are also available.

Programming

The following programming options are available for wireless DGP devices:

DGP number

Range: 1 to 15

Specify the DGP address that this wireless DGP will use in the Alliance system. This should be the same as the address specified in *DGP programming* for this controller (see *DGP number* on page 122).

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

DGP mode

Specify the number of zones the DGP supports and consequently the number of DGP addresses the DGP takes up in the system. DGP modes include the following:

Standard, 29 zones. Provides 29 wireless zones and consumes two DGP addresses. Zones 1, 2, and 3 are used to transmit up to 29 device tamper, supervision fail, and battery low events as a single global event.

Standard, 13 zones. Provides 13 wireless zones and consumes one DGP address. Zones 1, 2, and 3 are used to transmit up to 13 device tamper, supervision fail, and battery low events as a single global event.

Extended, 32 zones. Provides 32 wireless zones and consumes two DGP addresses. Enables all 32 zones with device tamper, supervision fail, and battery low events to be handled transparently by protocol.

Extended, 16 zones. Provides 16 wireless zones and consumes one DGP address. Enables all 16 zones with device tamper, supervision fail and battery low events to be handled transparently by protocol.

Supervision time

Range: 1 to 32 hours

Set the time period for testing the supervision flags of all active sensors.

Back tamper

Enable or disable the back tamper switch on the DGP.

Serial number

Specify the serial number for the sensor. The serial number is preset in the wireless sensor during manufacturing and identifies each sensor to the DGP to enable communication between the DGP and the sensor. For convenience, the serial number is presented in HEX notation with digits 0 to 9 and characters A, B, C, D, E and F.

Sensor type

Specify the sensor type. The sensor type is preset in the wireless sensor during manufacturing and defines the style of sensor being used. When programming the sensor type value, ensure that the reported sensor type is consistent with the device being programmed. *Table 8* shows the available sensor types.

Table 8. Sensor types

Type	Description
1	Bill trap
2	Smoke detector
3	Panic
4	PIR
5	Recessed door window sensor
6	Thermal detector
7	Carbon monoxide sensor
8	Not assigned
9	Glassbreak/shock sensor
10	Door window sensor
11	1 or 2-button panic sensor
12	Fire pull
13	Glass guard
14	Freeze sensor
15	2 or 4-button key fob
16	Not assigned
17	Not assigned
18	Supervised interior siren
19	4-point sensor
20 to 31	Not assigned

Sensors that are currently supported by the Alliance wireless DGP are listed in *Table 9*.

Table 9. Sensors supported by Alliance wireless DGP

ITI stock code	Sensor type
60-707-0195R	2-button SAW keychain touchpad
60-670-95R	SAW door/window sensor
60-741-95	Recessed micro door/window sensor
60-639-95R	SAW PIR motion sensor
60-873-95	Wireless ShatterPro glassbreak sensor
60-578-10-95	Water-resistant pendant panic sensor

Wireless devices zone numbering

When a wireless device is added to a wireless DGP, the device is assigned up to four system zone numbers. The number of zones assigned depends on the type of device. For example, the 4-point sensor should have all four zones assigned. Each wireless DGP has from 13 to 32 zones allocated, depending on the DGP mode programmed. The system zone number assigned to the wireless device is based on both the DGP system address (see *Numbering* on page 324) and the number of zones assigned to the device.

Example 1. The wireless device is allocated 1 zone and is the first device being programmed. The wireless DGP system address is DGP 2 with a zone range of 33 to 48. The associated zone number for the device will be 33.

Example 2. The wireless device is allocated 2 zones and is the second device being programmed. The wireless DGP system address is DGP 2 with a zone range of 33 to 48. The associated zone numbers for the device will be 34 and 35.

Example 3. The wireless device is allocated 1 zone and is the third device being programmed. The wireless DGP system address is DGP 2 with the zone range of 33 to 48. The associated zone number for the device will be 36.

Supervision flag

Supervision options set the supervision mode for each zone. Supervision may be controlled by the first relay of each DGP. For example, relay 17 would control the supervision for DGP 1. The following supervision flags are available:

Enabled. Supervision is enabled.

Disabled. Supervision is disabled.

Relay controlled. Supervision is controlled by the state of the first relay number for the wireless DGP. For example, relay 17 for DGP 1.

Key fob programming

Each wireless DGP supports up to 16 key fob devices. Depending on the type, each key fob will have two or four buttons which offer the options shown in *Table 10*.

Table 10. Key fob options

Key fob button function	Description
User	When the button is pressed, the assigned user number will arm/disarm the system.
Relay	When the button is pressed, the assigned relay is activated/deactivated.
Unused	The button is not used.

Serial number

The sensor serial number specifies the sensor that the fob will trip when activated.

Chapter 7 Door programming features

This chapter provides an overview of doors and door programming features.

In this chapter:

Doors

Doors are one of the most important concepts to understand within the Alliance system. The terminology dealing with doors can present difficulties to installers and lead to confusion. Although most systems define doors as keypad/card-reader devices (RAS devices), the Alliance system supports a maximum of 64 doors in a combination of up to 16 RAS devices and 48 intelligent doors.

System bus RAS devices are:

- Configured in the arming station
- Considered doors only in door group programming and assigned a door number between 1 and 16 that reflects the RAS device's system bus address

Intelligentdoors are:

- Comprised of one to four RAS devices per door connected to a 4-door/elevator controller
- Configured in door programming
- Assigned door numbers between 17 and 64 in door access programming

Another significant difference between a system bus RAS device and a door is the physical connection itself. The system bus uses a proprietary bus format, so non-Alliance devices require an AL-1170 module interface. For example, it is impossible to add a standard Wiegand reader directly on the system bus (it must be connected to an AL-1170), while the 4-door controller provides each door with a dedicated reader port that is capable of accepting either an Alliance or non-Alliance reader device directly. There is no need to add an AL-1170 when connecting a Wiegand reader to the 4-door controller's reader port. In fact, you can view the reader port as an onboard AL-1170.

The four reader ports located on the 4-door/elevator controller are, by default, the IN readers for the door. Each of these four doors has one reader port assigned. The reader ports have the following assignments:

- Reader Port 1: Assigned bus address 1 (RAS 1).
- Reader Port 2: Assigned bus address 2 (RAS 2).
- Reader Port 3: Assigned bus address 3 (RAS 3).
- Reader Port 4: Assigned bus address 4 (RAS 4).

Some devices, such as Wiegand readers, do not have provisions for bus addresses. Therefore, when configuring RAS devices within a 4-door controller, the first four RAS

numbers correspond to the reader ports. The reader port number follows the RAS number/ address.

Door/RAS numbering

Table 11 shows the door/RAS numbering scheme.

Table 11. Door/RAS numbering scheme

Door number	IN RAS address	IN RAS address	OUT RAS address	OUT RAS address
1st Door	1 or (Reader Port 1)	5	9	13
2nd Door	2 or (Reader Port 2)	6	10	14
3rd Door	3 or (Reader Port 3)	7	11	15
4th Door	4 or (Reader Port 4)	8	12	16

Functions

Doors can be used for the following functions:

Onboard relays. Each door can directly access one of the four onboard relays on the 4-door controller. Under most circumstances, this relay is assigned the unlock relay.

Onboard zones. Each door can directly access up to four onboard zones on the 4-door controller. These zones will typically be used to support the controller's intelligent features.

Up to four reader devices. Each door is comprised of one to four reader devices, depending on required functionality.

Shunt support. Each door supports one of several zone shunt options.

Region control. Each door supports region control through antipassback.

Hardware timers. Each door provides several dedicated timers, for use with shunts, door unlocking, and extended access.

Request to exit (RTE). Each door supports a dedicated RTE function.

Alarm control. An alarm group is assigned to each door, defining arm/disarm behavior.

Advanced reader support. Each door supports numerous different reader types, such as Wiegand and Alliance smart card. The same holds true for card formats. Each door also provides numerous LED options.

Keypad/reader interface. The 4-door controller has its own local bus, supporting the full range of RAS devices. In addition, the 4-door controller also provides four reader ports, which can directly interface with Wiegand readers or Alliance readers; therefore, it is not necessary to equip each reader with AL-1170 interface boards.

Door-open-too-long (DOTL). Each door supports a DOTL function.

Door access programming

The following door access programming options are available for doors:

Door number

Range: 17 to 64

Specify which door is being programmed.The door number is based on the 4-door controller DGP address, as well as the logical door number. For example, a 4-door controller with an address of 1 would yield doors 17 to 20, where door 17 maps to Door 1, door 18 maps to Door 2, etc.

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Unlock time

Range: 0 to 255 (seconds)

Specify the amount of time the door unlocks when a user is granted access. This value is the total number of seconds the unlock relay will remain active.

Extended access time

Range: 0 to 255 (seconds)

Specify the amount of time the door unlocks when a user with extended access is granted access. This value is the total number of seconds the unlock relay will remain active. This option is useful when additional time should be granted to special users to meet ADA requirements.

Door shunt option

Specify one of several different door-shunting options. Door shunting is the ability to bypass an open door that might ordinarily generate an alarm.The door will remain shunted for the period of time defined in the *shunt time* option. Door shunt options include:

No shunting. The door is not shunted.

Zone shunting. The door is shunted for the specified shunt time. If the door is left open longer than the shunt time, an alarm is generated based on the zone type.

Zone shunting and DOTL. The door is shunted for the specified shunt time. If the door is left open longer than the shunt time, a DOTL (door open too long) alarm is generated. Enables forced door and DOTL to be reported on separate zone numbers.

Autoshunting and DOTL. If the area assigned to the door is disarmed, shunting of the door begins when the door zone is active (no code or card required). Enables forced door and DOTL to be reported on separate zone numbers.

Shunt time

Range: 0 to 255 (seconds)

Specify the amount of time the door can be open when a user is granted access without generating an alarm. This value is the total number of seconds user has to pass through the door, and shuts it again.

Extended shunt time

Range: 0 to 255 (seconds)

Specify the amount of time the door is can be open when a user with extended access is granted access. This option is useful when additional time should be granted to special users to meet ADA requirements.

Warning time

Range: 0 to -255 (seconds)

Specify the amount of time for a relay to activate before the shunt/extended shunt time expires.

Low security time zone

Range: 0 to 24

Define the hard time zone which, when valid, only requires a valid card/PIN to open the door. When the time zone is invalid and the *card + PIN IN reader* or *card + PIN OUT reader* option is enabled, a valid card **and** PIN is required in order to open the door.

IN/OUT region

Range: 0 to 254

Establish a region for either the IN or OUT reader, where the number corresponds to a previously configured region. The region defines a boundary for the assigned reader. When a user is granted access to a door configured with a region, the region number is recorded against the user code; therefore, when regions are employed with certain antipassback settings, the user could be denied access at the same reader twice. As soon as the user passes through the OUT region, the user is cleared from that region. If hard antipassback were enabled, the user would then be able to re-enter the region.

Note: *Region 0 acts as **Off Premises** while region 255 is used for **Region Disabled**.*

Passback

Define region behavior for the IN and OUT readers. Depending on the setting, the system will either grant or deny a user access to the same region twice in succession.

To clear a hard antipassback violation, the user must pass through another keypad/reader in order to change the region number that has been recorded against the user number or the card must be reprogrammed in the User menu. The region record is reset when the user is downloaded into the 4-door controller.

The door must be opened after the reader is used before antipassback will take effect. The door contacts **must** be wired to the 4-door controller.

Regions must be programmed for the IN/OUT regions in order for this option to function. Passback choices include:

No antipassback. No control for passback. A valid card/PIN opens the door without generating an alarm. Entering a region twice without leaving is possible.

Soft antipassback. A valid card/PIN opens the door when used to enter the region the second time without leaving the first, but a report is generated.

Hard antipassback. A valid card/PIN does **not** open the door when used to enter the region a second time without leaving the first. A report is generated.

Door options

Card plus PIN IN reader	**Enabled:** In order to open the door from the IN reader, the user must badge their card **and** enter their PIN on the keypad. **Disabled:** In order to open the door from the IN reader, the user must either badge their card **or** enter their PIN on the keypad.
Card plus PIN OUT reader	**Enabled:** In order to open the door from the OUT reader, the user must badge their card **and** enter their PIN on the keypad. **Disabled:** In order to open the door from the OUT reader, the user must either badge their card **or** enter their PIN on the keypad.
IN reader no PIN if time zone	**Enabled:** In order to open the door from the IN reader during the low security time zone, only a valid card is required. **Disabled:** In order to open the door from the IN reader during the low security time zone, a valid card **or** a valid PIN is required.
OUT reader no PIN if time zone	**Enabled:** In order to open the door from the OUT reader during the low security time zone, only a valid card is required. **Disabled:** In order to open the door from the OUT reader during the low security time zone, a valid card **or** a valid PIN is required.
Two cards IN reader	**Enabled:** In order to open the door from the IN reader, two different users need to present their card/PIN in the *2 card time* option in *4-door controller programming* (see *Two card time* on page 126). **Disabled:** In order to open the door from the IN reader, only 1 user is needed to present their card/PIN.
Two cards OUT reader	**Enabled:** In order to open the door from the OUT reader, two different users need to present their card/PIN in the *2 card time* option in *4-door controller programming* (see *Two card time* on page 126). **Disabled:** In order to open the door from the OUT reader, only 1 user is needed to present their card/PIN.
IN reader bypass region 0 users	**Enabled:** In order to open the door from the IN reader, the user must already be in a defined region. **Disabled:** Users with region 0 will be granted access to the IN reader. In most cases, region 0 is understood to be *off premises*.
OUT reader bypass region 0 users	**Enabled:** In order to open the door from the OUT reader, the user must already be in a defined region. **Disabled:** Users with region 0 will be granted access to the OUT reader. In most cases, region 0 is understood to be *off premises*.

Shunt until door closed	**Enabled:** Shunt the defined zones as programmed in the *shunt zones* option in *Door hardware programming* (see *Shunt zones* on page 155) until the door is closed. When the door is opened and the shunt is not active, the zone will generate an alarm. **Disabled:** The shunt timer will be used.
Cancel shunt after door secures	**Enabled:** Shunt the defined zones as programmed in the *shunt zones* option in *Door hardware programming* (see *Shunt zones* on page 155) until the door is closed. Opening the door again within the shunt time is not possible, and will generate an alarm. **Disabled:** The shunt timer will be used and the door can be reopened during the shunt time.

Door request-to-exit (RTE) programming

The following programming options are available for the door request-to-exit feature:

RTE time zone

Range: 0 to 24

Define a valid time in which a RTE (request-to-exit) button will unlock and/or shunt a door in order to allow exiting. When the time zone is valid, pressing the RTE button will unlock and/or shunt the door; if the time zone is not valid, pressing the RTE button will not unlock and/or shunt the door.

RTE

Define the RTE (request-to-exit) behavior by choosing one of the following:

RTE timed. When the RTE button is pressed, the door unlocks for the unlock time.

RTE held. As long as the RTE button is pressed, the door is held unlocked for as long as the unlock time or the button continues to be pressed, whichever is longer.

RTE only shunts. When the RTE button is pressed, the zone is shunted, but the door does not open.

RTE options

IN RTE disabled when armed	**Enabled:** The RTE button does not unlock the IN door if any of the areas assigned to the door are armed. **Disabled:** The RTE button unlocks the IN door regardless of the status of the areas assigned to the door. The RTE button must be wired to the 4-door controller. Area assignments are made in the *Area* option in *Door hardware programming* (see *Areas* on page 156).
OUT RTE disabled when armed	**Enabled:** The RTE button does not unlock the OUT door if any of the areas assigned to the door are armed. **Disabled:** The RTE button unlocks the OUT door regardless of the status of the areas assigned to the door. The RTE button must be wired to the 4-door controller. Area assignments are made in the *Area* option in *Door hardware programming* (see *Areas* on page 156).
Request-to-exit reporting	**Enabled:** When RTE zone is active, a report is generated and sent to both the printer and management software. **Disabled:** No report is generated.

Door alarm control programming

The following programming options are available for the door alarm control feature:

Alarm group

Range: 1 to 138

Define arm/disarm behavior for the door. The time zone defines when alarm control can be made. Alarm control is governed by alarm group attributes such as the *disarm only* option in *Alarm group programming*.

Alarm

Specify the type of alarm control available for the door from the following choices:

No alarm control. Arm/disarm is disabled for the reader.

Alarm control on first badge. Areas are disarmed on the first badge if access granted. Badging three times will arm the areas.

Alarm control on third badge. Areas are armed/disarmed on the third badge if access granted.

Alarm control with button I/F. Not supported

Alarm always (disarm = IN, arm = OUT). If access is granted at the IN reader, areas defined within the alarm group are disarmed. If access is granted at the OUT reader, areas defined within the alarm group are armed.

Authorized RAS

Range: 0 to 16 (these are system bus RAS devices)

This option supports the ability to provide a user interface to the door controller reader. It assumes the specified RAS is an LCD keypad. For example, when a user badges their card, the specified LCD keypad provides alarm control options, such as arm/disarm.

The RAS must have *toggle area status* in *RAS programming* (see *RAS options* on page 116) enabled in order to function.

IN/OUT denied if area armed

Prevent a user opening a door using the IN/OUT reader when any of the areas assigned to the door are armed. If enabled, a valid card/PIN will not open a door if any of the areas assigned to the door are armed. If disabled, the door will open regardless of the area's armed status.

The areas mentioned here do **not** come from the alarm group; rather, they come from the areas listed in the *Area* option in *Door hardware programming* (see *Areas* on page 156).

Door reader programming

The following programming options are available for the door reader feature:

Cardformat

Specify the card/key/token/reader data format when not using IUM memory. *Table 12* describes the various formats.

Table 12. Card formats

Format	Description
Wiegand 27-bit	For Indala ESP range of proximity readers supplied by Aritech
Aritech ASC	For AL-1191 proximity readers.
Kastle 32-bit	Kastle format cards.
Wiegand 26-bit	For standard 26-bit Wiegand format readers, including Wiegand swipe readers supplied by Alliance. Have a 16-bit card number (0-65534) and an 8-bit system code (0-255).
Indala ASC 27-bit	For Indala ASP range of proximity readers using 27 bit Wiegand format.
Indala ASC 26-bit	Not used in Europe.
Wiegand 32-bit	For 32-bit Wiegand format readers. Uses a 16-bit card number and 16-bit system code.
Mag. Card Alliance	For Alliance format magnetic swipe cards.
Mag. Card Midas	For Midas format magnetic swipe cards.
C36-bit	For C36-bit format.
Wiegand 30-bit	For Wiegand 30-bit format.
Wiegand 32-bit	For Wiegand 32-bit format.

Override time zone

Range: 0 to 24

Specify the time in which the door will unlock. When the time zone is valid, free access is allowed.

LED

Specify how the reader displays the status LED. *Table 13* describes the LED status options.

Table 13. LED status options

LED	Description
LED on when door locked	The LED turns on when the door is locked
LED on when door unlocked	The LED turns on when the door is unlocked
LED on when area armed	The LED indicates if the area assigned to the door is armed. If more than one area is assigned, all areas must be armed before the LED changes.
LED on when area disarmed	The LED indicates if the area assigned to the door is disarmed. If more than one area is assigned, all areas must be disarmed before the LED changes.
Two LEDs disarmed/armed	Readers with dual LED control lines connected indicate the area disarmed and armed with different color LEDs.
Two LEDs valid/void	Readers with dual LED control lines connected indicate user valid or void with different color LEDs.
No LED	No LED control.

Note: *On readers with dual LED control lines, the second LED can be programmed to indicate other conditions in DGP macro logic programming.*

Reader options

Hold door unlocked	**Enabled:** The door lock will not relock until the door is closed. **Disabled:** The door lock will relock, regardless of the door being open or closed, after the unlock time expires.
Unlock time zone after entry	**Enabled:** Before the override time zone unlocks the door, a user needs to enter the area. **Disabled:** Automatic unlock will start at the override time zone's start time.
Log door open/close	**Enabled:** When the door contact zone goes active then back to normal (a door is opened/closed), a report is sent to both the printer and management software. **Disabled:** Depending on zone type, no report is generated unless an alarm occurs.
Report forced door	**Enabled:** When the door is forced open without a valid card/PIN, a report is sent to both the printer and management software. **Disabled:** Depending on zone type, no report is generated unless an alarm occurs.
Hold door unlocked until door opens	**Enabled:** When a user is granted access at a door, the door relay will stay active until the door contact zone goes from active to normal (a door is opened/closed). **Disabled:** The door relay will perform normally.
Report door closed and locked	**Enabled:** When a door is closed AND locked, a report is sent to both the printer and management software. **Disabled:** Depending on zone type, no report is generated unless an alarm occurs.
LogDOTL	**Enabled:** When the door remains open after the shunt timer expires, a DOTL (door-open-too-long) report is sent to both the printer and management software. **Disabled:** Depending on zone type, no report is generated unless an alarm occurs.
Time attendance reader	Not Supported

Pulsed lock and unlock output	**Enabled:** Special lock strike opening is enabled. Two separate relays are pulsed at different times. **Disabled:** Normal lock strike opening. This option should only be enabled on locks that require two separate relays to be pulsed at different times in order to open and two separate zones for monitoring.
Disable duress	**Enabled:** Duress functionality is disabled for this door. **Disabled:** Duress functionality is enabled for this door.
Map open/unlocked to unlocked	**Enabled:** When the door is unlocked, an unlocked report is sent to both the printer and management software. **Disabled**: Unlocking is not reported. An unlock condition exists if the door is not closed **and** is locked.

Door hardware programming

All zones and relays used in this section are required to come from on board the 4-door/elevator controller. Any onboard zones set to zone type 0 (Disabled), in the *zone type* option in *Zone programming*, revert to being normal DGP system zones. Any zones assigned as door contacts or DOTL (door-open-too-long) must be assigned a zone type so that the control panel responds to generated alarms.

The following programming options are available for door hardware:

Unlock relay

Range: (depends on 4-door/elevator controller address and door number)

Specify the relay that is activated when a user is granted access and the door is unlocked.

DOTL relay

Range: (depends on 4-door/elevator controller address and door number)

Specify the relay that is activated when the DOTL (door-open-too-long) zone is active, due to the shunt timer expiring.

Forced relay

Range: (depends on 4-door/elevator controller address and door number)

Specify the relay that is activated when the door contact zone is active without the system having granted access (a forced door condition).

Warning relay

Range: (depends on 4-door/elevator controller address and door number)

Specify the relay that is activated (during the warning time) when the shunt timer is about to expire. For example, a separate buzzer might be tied to this relay in order to let the user know that the door needs to be closed.

Fault relay

Unsupported at this time.

RTE zone

Range: (depends on 4-door/elevator controller address and door number)

Specify the zone that activates the RTE (request-to-exit) function.

DOTL zone

Range: (depends on 4-door/elevator controller address and door number)

Specify the zone used to report a DOTL (door-open-too-long) condition.

Door contact zone

Range: (depends on 4-door/elevator controller address and door number)

Specify the zone used for the door contact. This zone lets the 4-door/elevator controller know when a door is opened/closed, especially during a forced door condition.

Monitor second door zone

Range: (depends on 4-door/elevator controller address and door number)

If enabled, the system will treat the spare zone as a second door contact; otherwise, the spare zone is available for other purposes.

Shunt zones

Specify which zones, assigned to the current door, require shunting. This zone is typically the door contact zone.

Interlock zones

Specify which door contact zones should be used in order to prevent doors from being accessed at the same time when door are on separate door controllers.

For example, to interlock Door 1 with Door 2, a contact on Door 2 must be wired to the spare zone on Door 1, and a contact on Door 1 must be wired to the spare zone on Door 2. The spare zone becomes the interlocking zone.

If a zone is being used for interlocking and no other door uses it for the door contact zone (this should be the case), then the 4-door/elevator controller will insert a 2-second delay before opening the door in order to allow for settling times.

A maximum of eight zones can be used for interlocking.

Areas

Specify the areas used by the door reader's *LED options*, *alarm control*, *entry denied if area armed*, and *IN/OUT RTE disabled*. The 4-door/elevator controller will look at the specified areas when requesting status information from the control panel.

It is important to remember that the areas specified here are not used for area control. The purpose of this option is to enable the 4-door/elevator controller to identify the status of areas and know whether or not to send an arm/disarm command to the control panel.

The alarm groups specified in *Door alarm control programming* will dictate which areas have alarm control, not the areas specified here.

Door/floor groups

Door and floor groups are programmed using an Alliance management software program, they are not programmed in Alliance Builder. These groups dictate when access is granted to 4-floor controller floors (1 to 64) and 4-door controller intelligent doors (1 to 64). Each device within the door/floor group may have unique time zones assigned.

The door group considers all RAS/intelligent doors as simply *doors*. RAS devices connected to the system bus (1 to 16) are configured in RAS Programming, while all other RAS devices that make up intelligent doors (17 to 64) are configured in Door Programming.

*W*hen a door/floor group is added or programmed, the system will automatically populate the door/floor list with all known doors/floors (system RAS devices and intelligent doors/floors).

Functions

Door/floor groups can be used for the following functions:

Assign unique times. Each RAS device that appears in the door group allows unique hard/soft time zone assignment.

User assignment. Door/floor groups are assigned to users in order to grant access. Failure to assign a user any door/floor groups would result in the user being unable to access any doors/floors. Furthermore, an invalid time zone would also deny access.

Programming

The following programming options are available for door/floor groups:

Door/floor group number

Range: 1 to 128 (without memory expansion the range is 1 to 10)

Specify which door/floor group is being programmed.

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Doors/floors

Specify the following:

Door/floor number. The assigned system bus RAS (range 1 to 16) intelligent door (range 17 to 64) or floor (range 1 to 64) address/number.

Door/floor description. The door/floor description, taken from either the RAS device, or door/floor programming sections.

Time zone. Specifies the time period access will be granted for this door/floor. The range is 1 to 41.

Note: **Note:** Only system RAS devices (1 to 16) can be assigned a soft time zone, range 26 to 41. Floors cannot be assigned a soft time zone.

Time zone description. Programmed in *Hard time zone Description* on page 227 or *Soft time zone Description* on page 234.

Chapter 8 Control panel programming features

This chapter provides an overview of control panels and control panel programming features.

In this chapter:

Control panel

The Alliance system is based on the Alliance control panel. The control panel is responsible for managing the vast majority of the security system. The control panel:

- Communicates with all system bus devices, ensuring that the devices are responding correctly, as well as gathering status information
- Maintains user database and associated databases
- Communicates to PC management software through a variety of physical mediums, such as RS232 and PSTN
- Provides expandable resources, such as users and alarm groups, through memory modules
- Reports alarms to central stations through on-board dialers
- Controls hardware, such as opening doors and bypassing zones
- Supports external printers added to the control panel through additional board interfaces mounted on the panel, allowing certain events to be logged in real-time
- The control panel maintains the vast majority of programming options available. For example, the control panel handles adding/removing keypads to the system bus via keypad/management software. See *RAS (remote arming stations)* on page 112.

Control panel features

Table 14 shows the features provided by the Alliance control panels.

Table 14. Control panel features

Feature	AL-4X17	AL-3017	AL-2017
Areas	16	16	16
Maximum number of zones	256	64	32
Number of 8-zone expanders supported directly on control panel	2	2	2
Maximum number of relays	255	255	255
Maximum number of doors	48	48	0
Maximum number of DGPs	15	15	15
Maximum number of system bus RAS devices	16	16	16
Default number of alarm groups	32	32	32
Default number of door groups	10	10	10
Default number of floor groups	10	10	0
Expandable memory support	Yes	Yes	No
Clock relay controllers support	Yes	Yes	Yes
Number of card holders	50	50	50
Number of users with names	50	50	50
Number of users with PIN	50	50	50
Access logged events	10	10	10
Alarm logged events	250	250	250
Onboard zones	16	8	8
Onboard relays (physical and virtual)	5	5	5

Memory expansion

The ability to support a larger number of resources is dictated by the attached memory module. *Table 15* shows the available memory modules and their respective limits.

Table 15. Memory modules

Memory related resource	1 MB (non IUM)	4 MB IUM	8 MB IUM
Door groups	128	128	128
Alarm groups	138	138	138
Floor groups	128	128	128
Logged alarm events	1000	1000	1000
Logged access events	1000	1000	1000
Card holder users	11466	17873	65535
Users with names	200	200	200
Users with PIN	1000	1000	1000

Note: *Memory expansion must be paired between control panels and 4-door controllers. For example, adding a 4 MB IUM on the control panel requires adding the same memory type for all 4-door controllers.*

IUM, not only increases the number of resources, but also expands the card data from 26 bits to 48 bits.

When upgrading a control panel with an IUM, first do a full upload of the control panel to the management software in order to back up the system. Next, install the IUMs on both the control panel and all 4-door/elevator controllers (they must be paired). Reset the control panel by using the *Kill Jumper*. Go back to the saved system and select the appropriate IUM and download the system back to the control panel.

Multiple panel systems

A multiple panel system is defined as an Alliance system containing more than one control panel. If a significant number of resources, such as doors and zones, are required, the panels may be networked. Although a maximum of sixteen control panels may be networked within a single system, the maximum recommended number due to real-world performance, is seven. The ability to network multiple control panels within a single system is facilitated by RS485 to RS232 interface converter ancillary boards.

Communications

Communications between the outside world and the control panel occur over the RS232 or PSTN. In the case of PSTN, the control panel must have the on-board dialer configured with the appropriate telephone lines, while the RS232 option requires outfitting the control panel with an optional Computer/Printer Interface Module.

Printing

As events occur, they can be logged to an optional printer. The printer is connected to the control panel through optional interface boards, such as the Computer/Printer Interface Module.

Functions

Control panels can be used for the following functions:

RAS/DGP communication. All RAS/DGP devices communicate with the control panel over the system bus. These devices obtain data from the control panel, provide status information, as well as generate alarms.

Software communications. Alliance management software communicates directly with the control panel in order to monitor events, perform device control (i.e. unlock doors), and program users. This is accomplished over several communications options, including RS232 and PSTN.

User database. Authorized users are stored within the control panel. RAS devices connected to the system bus will obtain authorization when a PIN/card is presented from the control panel.

Smart card devices will buffer a limited number of users in their respective memory. In the event a bus failure occurs, a card is likely to function.

RAS devices attached to 4-door controllers obtain user information from the door controller, rather than the control panel (redundant user database).

Resources. The memory module attached to the control panel defines the maximum number of programming elements.

Multiple panel configurations. Each control panel is assigned a unique address identifier. This address is used when configuring systems containing more than one control panel.

Programming

The following programming options are available for control panels:

Control panel number

Range: 1 to 7

Specify the control panel number.

Note: *The total number of control panels allowed per system is less than the specification in order to account for latency issues.*

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Model

Specify the control panel model. The selected model will dictate the overall capabilities and limits of the system.

Memory

Specify the memory module attached to the control panel.

Note: *Memory expansion must be paired between control panels and all 4-door/elevator controllers.*

Address

Assign a unique address for each control panel within a system. Although the control panel address is only programmed using the keypad, when management software programs create additional panels the database treats them as control panel 2, 3, etc.

Macro logic

Macro logic provides a tool for activating event flags when specific events occur. These events provide inputs to logic equations. When the result of the equation is true, the macro event tied to the equation will follow.

Up to four event flag inputs may be included in the logic equation. Each macro input in the logic equation can be programmed as an AND or an OR function and may be inverted.

Options are provided so that the macro's result will trigger a macro output which may be a pulse, timed, on delay, off delay, or latched when activated.

The event flags used here are pre-defined event flag numbers as listed in the macro event flags. Some can only be used for macro inputs, some for macro outputs, and some may be used for both. Before programming a macro, it is important to understand the basics of Boolean logic. For information on Boolean logic, see *Boolean logic* on page 278.

Alliance system macros

Both control panels and 4-door/elevator controllers have programmable macros. The following are basic elements of a macro with their attributes:

Macro. Number and description

Four inputs. Event flag number or relay number

Logical equation. AND (NAND) or OR (NOR)

Timing. Pulse, delay ON, delay OFF, or latched

Output. Event flat number or zone number

Macro logic number

Range: Control panel 1 to 24, 4-door/elevator controller 1 to 48

Identifies the macro or program number.

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Input

Range: 1 to 4

Provides input as an operand in the Boolean equation for the macro. Any input can be inverted prior to the gate operator.

Input type. The user can select the type of input for each of the four inputs. The state of the input defined in the input type can be inverted prior to the function.

Output

Defines the behavior and output type that, if the result of the equation is true, the macro will act on or active.

If the output type is allocated to a zone, the zone selected will not function. Because of this mode of operation, the zone number assigned may be a phantom zone, not physically available.

Unless inverted (NOT), the zone will be in an alarm condition when the macro activates and normal when the macro resets.

The output may be optionally inverted, the NOT function.

Output type. Identifies the type of output and what output will be acted on. Note that the output result has the inverted option.

Output function. The output function allows the user to define what type of output function will be activated by the macro as shown in *Table 16*.

Table 16. Output functions

Function name	Description
Disabled	Macro is disabled.
Non-timed	The output follows the result of the logic equation only. If an event flag or output for this macro changes, the logic equation will be calculated again.
Pulsed	Activates the output for the programmed time or the active period of the logic result whichever is the shortest. On pulse (1 to 255 seconds), on pulse (1 to 255 minutes)
Timed	Activates the output for the specified time period regardless of the macro output changing. On timed (1 to 255 seconds) on timed (1 to 255 minutes)
Delayed	Activates the output after the specified timer expires, unless the result of the logic equation is no longer valid. On delay (1 to 255 seconds), on delay (1 to 255 minutes)
Non-delayed	Follows the results of the logic equation, but remains active for the time programmed after the result of the logic equation is no longer active. Off delay (1 to 255 seconds), off delay (1 to 255 minutes)
Latched	When the output function is set to latched, the macro is not looking to the logical expressions OR or AND for all inputs. The first three inputs will be handled as SET inputs and the fourth input will be handled as a RESET input of a RS Flip-flop. The RESET will always predominate the SET inputs. Inverting the input conditions or output conditions is still applicable.

Output duration

Specify the time period applied to the output function. Only applicable for time-based output functions, such as timed and delay. The range is from 1 to 255 and the time period varies between seconds or minutes, depending on output function selected.

Printers

Printer programming not only configures a printer connected to the system, but also dictates how and when the printer will output events. In order to interface a printer to the control-panel, a printer/computer-printer interface board is required.

Programming

The following programming options are available for printers:

Printer type

Specify the type of printer connected to the interface board. *Table 17* details the printer types.

Table 17. Printer types

Printer type	Description
Epson	Baud: 9600, Word: 7 bit, Parity: Even, Stop: 1
Laser HPII	Baud: 9600, Word: 8 bit, Parity: None, Stop: 1
Laser HPII	Baud: 19200, Word: 8 bit, Parity: None, Stop: 1
Epson	Baud: 9600, Word: 7 bit, Parity: Odd, Stop: 1
Epson	Baud: 9600, Word: 7 bit, Parity: None, Stop: 1
Epson	Baud: 9600, Word: 8 bit, Parity: None, Stop: 1
Epson	Baud: 9600, Word: 8 bit, Parity: Odd, Stop: 1
Epson	Baud: 9600, Word: 8 bit, Parity: Even, Stop: 1

Printer time zone

Range: 0 to 64 (includes hard and soft time zones)

Specify the time zone when the printer is active.

Real-time printing

If enabled, the printer will print events as they occur; otherwise, they will not be printed.

Alarm events

If enabled, all alarm events will be printed; otherwise, they will not be printed.

Access control events

If enabled, all access control events will be printed; otherwise, they will not be printed.

Print outside of time zone

If enabled, the printer will only be active outside the specified time zone; otherwise, the printer is only active during the time zone.

Timers

Custom hardware timers can be triggered in the system by various events. When an event flag tied to one of the timers is raised, the system starts the timer, which runs for the specified time. When the timer elapses, the system generally performs other actions, such as arming or disarming an area.

Timers are system-wide, meaning other programming features make use of defined timers in order to determine how long a certain feature will be enabled or disabled. For example, RAS devices will open a door for the time defined in the *RAS unlock time* option.

In general, if some other programming feature refers to a period of time that is not defined within the scope of that feature, the time period will usually be defined in timer programming.

Note: *Timers are accurate to +/- 1 the value entered (a timer set for 20 seconds will fall between 19 and 21 seconds). Therefore, avoid using values of 1 second/minute.*

Functions

Timers can be used for the following functions:

Timed events. Use timers to program how long certain events and system states will be able to run.

Testing. Use timers to set a certain period of time in which the system can be tested without generating alarms.

System flexibility. Use timers to set an appropriate amount of time for users to perform actions without generating an alarm. For example, if a user required a door to stay unlocked for a significant amount of time, you can program the *door unlock time* to keep the door unlocked for the necessary amount of time without generating an alarm.

Programming

The following programming options are available for timers:

Alarm group restriction 1 to 7 disarmed time

Range: 0 to 255 (minutes)

Determine the amount of time the associated areas will be disarmed. After the specified amount of time has elapsed, the area will be automatically armed again. The alarm group restriction must be programmed for *timed disarm* in *Alarm group restriction programming* (see *Timed disarmed areas* on page 198) and be assigned to an alarm group for this timer to be used.

Program the individual times for each alarm group restriction (1 to 7) for the period of time the associated area should be disarmed. The associated area will be armed after the specified timer expires.

If the *Alarm group restriction disarmed time* is left at zero and the restriction is programmed for an alarm group, the associated area will not be rearmed.

The *Alarm group restriction disarmed time* will be overridden by the Area disarmed time if any time, but zero, has been programmed for the associated area.

If the alarm group restriction is being used in conjunction with *Autoarm/disarm programming*, the *Alarm group restriction disarm time* is the delayed arming time.

Disarm test time

Range: 0 to 255 (minutes)

Specify the time available to do a disarm test.

Arm test time

Range: 0 to 255 (minutes)

Specify the time available to do an arm test.

Warning time

Range: 0 to 255 (minutes)

Specify the duration of the warning time. When alarm group restrictions are used and areas are programmed for timed disarm, a warning will sound (if a warning time is programmed) indicating the areas are about to arm.

Delayed disarmed alarm time

Range: 0 to 255 (seconds)

Specify the delay time before an alarm from a delayed disarmed alarm is reported to the central station. The delay time is overridden if another delayed zone has already been activated.

Suspicion time

Range: 0 to 255 (seconds)

Specify the length of time that a camera continues to operate after a suspicion zone has switched to normal state.

Service time

Range: 0 to 255 (minutes)

Specify the amount of time a technician, who has been given service technician privileges, has to service the system.

Local alarm reminder time

Range: 0 to 255 (minutes)

Specify the time that can elapse between acknowledging a local alarm and an alarm reoccurring, including the audible alert.

Individual zone test time

Range: 0 to 255 (minutes)

Specify the maximum time required to perform a test on an individual zone.

RAS unlock time

Range: 0 to 255 (seconds)

Specify the amount of time a door's RAS device will be unlocked when the door's corresponding event flag has been triggered. This time applies to all system doors.

Testing event flag time

Range: 0 to 255 (seconds)

Specify the time the testing event flag is triggered to activate devices in order to perform an arm test. The event flag will only be triggered for half the programmed time. The remaining time is used to allow the device to switch back to the normal state.

External siren time

Range: 0 to 255 (minutes)

Specify the amount of time for the on board external siren drivers to activate.

Internal siren time

Range: 0 to 255 (minutes)

Specify the amount of time for the on board internal siren drivers to activate.

AC fail delay time

Range: 0 to 255 (minutes)

Specify the delay time before AC fail is reported to the central station. Enter the value *0* for no delay.

Sirens delay time

Range: 0 to 255 (minutes)

Specify the time that elapses before sirens cut-off after activation.

Reporting alarms delay time

Range: 0 to 255 (seconds)

Specify the delay time before a burglar alarm (BA) or BA class tamper alarm (TA) is reported to the central station. It can be used to prevent alarm reporting for users that have problems disarming their area in time. After a burglar alarm or input tamper activation, there will be a delay of the specified time before the burglar alarm (BA) or BA class tamper alarm (TA) will be reported to the central station. All other alarms are reported immediately, without delay.

A to B alarm delay time

Range: 0 to 255 (minutes)

Specify the delay time that the system waits for a second alarm. If the second alarm happens within the delay time, it will be reported as a verified alarm.

Screensaver timeout time

Range: 0 to 255 (seconds)

Specify the amount of time it takes for the RAS device screensaver to time out. The screensaver timer will be reset with the programmed period every time you press a RAS key when the screensaver is not active. To manually activate the screensaver, press the **CLEAR** key at the *Enter Code* prompt.

RAS card and PIN timeout

Range: 0 to 255 (seconds)

Specify the delay time between badging the card and entering the PIN.

Double-knock interval

Range: 0 to 255 (minutes)

If enabled for a particular zone, the double-knock interval specifies the maximum permitted time between a zone becoming active for the first time and becoming active for a second time. If the time a zone remains active exceeds the permitted time, an alarm condition is registered.

Double-knock duration

Range: 0 to 255 (seconds)

If enabled for a particular zone, the double-knock duration specifies the maximum permitted time a zone may remain active. If the time a zone remains active exceeds the permitted time, an alarm condition is registered. If this value is set to zero, an alarm is not generated by prolonged activation, but is determined by the double-knock interval.

Chapter 9 Access programming features

This chapter provides an overview of access programming features.

In this chapter:

Areas

An area defines a physical space within a building. The primary purpose of the area is to establish intrusion protection, facilitated through one or more zones, and to tie those zones to RAS devices (accomplished through alarm groups).

Each zone added to the system is assigned one or more areas. The zones controlled by RAS devices for the purpose of arming/disarming the area. Zones are not directly armed, rather their associated areas are. For example, when a user arms a specified area through a keypad, the system will treat all zones assigned to that area as being in the armed state. When an assigned zone enters the active state it will cause the system to generate an alarm.

Areas also define numerous event flags that may be used in performing other system functions. For example, you can assign specific event flags to be raised whenever the area is either armed or disarmed.

Areas also support several central station reporting options. When an alarm is generated, the system will use the *Reporting options* on page 181 in order to determine which central station to call.

Functions

Areas can be used for the following functions:

Intrusion. Zones can be assigned to a combination of areas, in order to provide intrusion control.

Reporting. Areas define which central stations should be called in the event an alarm is generated for that area.

Arm/disarm. Zones assigned to an area can be armed/disarmed through a RAS device (keypad/card reader).

Entry/exit. Areas define timers that allow specified periods of time to elapse before generating an alarm when the system is armed/disarmed.

Event flags. Each area supports numerous event flags that can be used by other programming options, such as system macros.

Text words. The area name is stored as a system text word in the control-panel that can be seen in the RAS devices.

Programming

The following programming options are available for areas:

Area Number

Range: 1 to 16

Specify the area to program.

Name

Range: Up to 16 characters

Specify the name given to the area. The name is converted into a system text word, and is transferred to the control panel. As a result, the name will appear within RAS keypad devices.

Since the system only allows up to 100 user-defined text words, try to reuse existing text words in the *Text word library* on page 308.

Entry time

Range: 0 to 255 (seconds)

When entering an armed area containing entry/exit zones, the entry timer should be set to permit the user ample time to disarm the system before generating an alarm. Each area supports one entry timer.

Entry/exit zones are defined as zone types 3 (entry/exit alarm), 4 (access zone), 13 (entry/exit without arm check), 14 (access without arm check), 41 (entry/exit emergency door), and 42 (entry/exit emergency door with code). However, the timer will only start with zone types 3, 13, 41, and 42.

If zones are assigned to more than one area, the longest entry/exit time is used. The entry time must be more than 10 seconds. The default is set at 30 seconds.

Exit time

Range: 0 to 255 (seconds)

When exiting an area that has been armed containing entry/exit zones, the exit timer will start in order to give the user ample time to leave the premises before generating an alarm. Each area supports one exit timer.

If zones are assigned to more than one area, the longest entry/exit time is used.

Key box timer

Range: 0 to 255 (minutes)

The key box timer determines the exit time by the duration specified in minutes. Immediately after the exit timer expires, the key box timer starts. Before this additional key box timer expires the zone must be closed. If it is not closed, a full alarm will be triggered again even if the previous trigger was also an alarm. During the exit timer and key box timer, openings and closings will not be registered and will not generate an alarm.

Area disarmed time

Range: 0 to 255 (minutes)

When using alarm group restrictions, the restriction provides an option to disarm the area for a specified period of time. Under normal circumstances, this time comes from programming in *Timers* on page 171. If the time is set in this option to any value other than zero, it will override the value programmed in Timers programming.

If the *alarm group restriction disarmed time* in *Timers programming* is set to zero in order to specify that the area will not rearm, the time set here will apply for the area.

Reporting options

Report to central station 1	**Enabled:** Reports opening/closing and late-to-close access events to central station 1. **Disabled:** Does not report to central station 1.
Report to central station 2	**Enabled:** Reports opening/closing and late-to-close access events to central station 2. **Disabled:** Does not report to central station 2.
Report to central station 3	**Enabled:** Reports opening/closing and late-to-close access events to central station 3. **Disabled:** Does not report to central station 3.
Report to central station 4	**Enabled:** Reports opening/closing and late-to-close access events to central station 4. **Disabled:** Does not report to central station 4.
Enable audio listen-in (Not supported in the US)	**Enabled:** Audio listen-in will be enabled. **Disabled:** Audio listen-in will be disabled.
Report exit faults	**Enabled:** On an exit fault a local alarm is generated and a special exit fault signal is reported to the central station. **Disabled:** Exit faults will not be reported to the central station.
Prevent arming if all zones bypassed	**Enabled:** The area cannot be armed if all zones in the area are bypassed. **Disabled:** The area can be armed if all zones in the area are bypassed.
Area disarm channel	Program the channel for a disarmed event with channel numbers 00 - 99 for each area. Leave blank to disable.
Area arm channel	Program the channel for an armed event with channel numbers 00 - 99 for each area. Leave blank to disable.

Event flags

External siren event flag	When the area is armed, the specified event flag is raised when a zone generates an alarm. This will cause the external siren to sound. The default is event flag 1.
Disarmed event flag	The specified event flag is raised when the area is disarmed.
Zone active event flag	The specified event flag is raised when a zone assigned to the area becomes active. Zones that can be used to change the status of an area, cameras, or unused zones, are excluded.
Bypass event flag	The specified event flag is raised when a zone assigned to the area has been bypassed.
Armed alarm event flag	The specified event flag is raised when the area is armed.
Disarmed alarm event flag	The specified event flag is raised when the area is disarmed.
Internal siren event flag	When the area is armed, the specified event flag is raised when any zone assigned to this area generates an alarm. This will cause the internal siren to sound. The default is event flag 13.
Exit event flag	The specified event flag is raised when the exit timer is running.
Entry event flag	The specified event flag is raised when the entry timer is running.
Local alarm event flag	The specified event flag is raised when emergency doors and 24-hour local alarm zone generate an alarm.
Warning event flag	The specified event flag is raised when an alarm group restriction timer is running and the area is about to be armed or a test mode is in progress and the test is about to end.
Camera event flag	The specified event flag is raised when a zone having the camera event generates an alarm, and the area is disarmed. The flag is used to control cameras.
Prealarm event flag	The specified event flag is raised when a delayed disarmed alarm zone is active and the delay time is running. Used to provide visual indication of a possible alarm. The event flag is only activated for the delayed period.

Out-of-hours time zone	The specified event flag is raised when an area is disarmed, when it should be armed. Generates a report if the area is disarmed while the area should be armed. The message reported depends on the type of transmission protocol. This option is commonly used in conjunction with *Auto arm/disarm programming*.
Antimask event flag	If an attempt to arm an area that has the anti-mask event flag set to a non-zero value and any inputs associated with this area are active, the event flag is set for 5 minutes. The antimask event flag is active for the duration of the timer and is reset when either the timer's time elapses or the area is successfully armed. This event flag is commonly used with PIR detectors with an anti-mask feature. An output is assigned to the anti-mask event flag that is wired to the detectors. When this output is activated, the detectors must be triggered by a walk test in order for them to become normal after the output is deactivated (after 5 minutes).
Latched reset event flag	This event flag is triggered when two valid disarm codes are entered within 5 minutes for an area and the area is disarmed. The event flag is set for 5 seconds. For an additional 4 seconds the zone 67 (latched detector) associated with the area is disabled for a total disabled time of 9 seconds. Zone 67 is a 24-hour alarm conditional bypass that is conditional on the 9-second timer.
Alarm A event flag	The specified event flag is raised when an area identifies a first alarm.
Alarm B event flag	The specified event flag is raised when an area identifies a second alarm.
Tamper alarm event flag	Unsupported

Area links programming

Area links support the ability to tie several areas together to create a common area. This will impact how the system handles arming and disarming as described below:

Arming. The common area will only arm when **all** linked areas have been armed.

Disarming. The common area will disarm when **any** linked area is disarmed.

For example, area 1 is defined as the common area, and is linked to areas 2, 3, and 4. When any of the linked areas (2, 3, or 4) are disarmed, area 1 (common) is disarmed. When all three linked areas are armed, the shared area will also be armed.

Each area will continue to have its own entry/exit times programmed in *Area programming*, regardless of the programmed area links.

Common area number

Range: 1 to 16

Specify the common area number.

Link to area

Specify the areas that should be linked to the common area.

Bank vault areas

Bank vault areas are areas designated for high security requirements. By specifying which of the 16 areas should be promoted to bank areas, the system will automatically arm all other bank vault areas after a preset delay. The delay time is based on the alarm group restriction timer and will only start when all bank vault areas are armed.

For example, a building has three office areas (areas 3, 4, and 5) along with two common areas (areas 1 and 2). The desired end result is to arm the common areas at a specified time **after** the last office area is armed. To accomplish this you would:

- Promote areas 3, 4, and 5 to bank vault areas.
- In Control panel options programming, set *Disable auto insert of alarm group restriction* to disabled (see *System options* on page 258). This will enable the bank vault areas feature.
- The common area are linked to bank vault areas 3, 4, and 5. This is programmed in Area links programming.
- Create an area group restriction in order to specify which common areas are included. In Alarm Group Restriction programming, enable areas 1 and 2 in the *Timed disarm area*s option (see *Timed disarmed areas* on page 198).
- To program the preset delay, specify the *Alarm group restriction disarmed time* value in Timers programming (see *Alarm group restriction 1 to 7 disarmed time* on page 172). The timer used is based on the alarm group restriction number used above.
- In order for this function to work properly, the alarm group must include the areas assigned to the alarm group restriction (areas 1 and 2).

Programming

The following programming options are available for bank vault areas:

Areas

Range: 1 to 16

Specify the areas to promote to bank vault areas.

Regions

Regions are used in establishing boundaries within 4-door/elevator controllers. The system allows you to assign regions to both the IN and OUT readers on the 4-door/elevator controller. When a user is granted access at a door, the user is assigned that particular region. When used in conjunction with *antipassback* programmed in *Door access programming* (see *Passback* on page 143), users can be prevented from accessing the same reader twice, or access may be granted but a report will be generated.

Functions

Regions can be used for the following functions:

Establish boundaries. Regions set up boundaries when used in conjunction with the antipassback feature. For example, a user can be denied access at the same reader they have already used to enter the region.

Monitor user location. When a user is granted access at a door supporting regions, the region number is added to the report.

Programming

The following programming options are available for regions.

Region number

Range: 0 to 255

Specify which region is being programmed.

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Chapter 10 Alarm control programming features

This chapter provides an overview of alarm control programming features.

In this chapter:

Alarm groups

Alarm groups define alarm control for the Alliance system. This impacts users, doors, zones, as well as RAS devices. An alarm group is assigned to each RAS device in the system and will dictate the areas the device/user has control over, the times the alarm group is valid, the menus that will be accessible (if the RAS is a keypad), and the functionality that is supported by the RAS device.

Alarm groups fall into two distinct categories:

User alarm group. The alarm group assigned to the user determines what alarm control capability, if any, the user is granted.

RAS and door alarm group. The alarm group assigned to the RAS or door device determines what alarm control capability is supported by the device.

When an alarm group is created, the user alarm group option will decide the category. This is why, under some programming options, the alarm group choices will be much shorter than the total number of groups defined for the entire system. For example, when adding a user to the system, the choice of alarm groups would be limited to only those groups with the user alarm group option enabled.

It is important to understand how the system resolves the capabilities of a user at a RAS device. For example, when a user approaches a RAS keypad and enters their PIN the keypad will compare the alarm group capabilities defined for the RAS keypad with the alarm group capabilities defined for the user. Only those capabilities that match between the two will be allowed. A RAS device that is not programmed to allow alarm control (based on the assigned alarm group) will not allow alarm control, even by a user with an alarm group with that capability.

Hard-coded alarm groups

The system, by default, provides the ten hard-coded alarm groups shown in *Table 18*.

Table 18. Hard-coded alarm groups

Number	Name	Description
1	No access	All user menu options disabled Cannot access any areas Assigned to users
2	Master RAS or door	All user menu options enabled Access to areas 1 to 16 All alarm group restrictions enabled Assigned to devices
3	Master code access	All user menu options enabled Access to areas 1 to 16 Assigned to devices
4	8-Area master RAS (1 to 8)	All user menu options enabled Access limited to areas 1 to 8 All alarm group restrictions enabled Assigned to devices
5	8-Area master RAS (9 to 16)	All user menu options enabled Access limited to areas 9 to 16 All alarm group restrictions enabled Assigned to devices
6	Master installer	All user menu options enabled Access to areas 1 to 16 No alarm control Assigned to devices
7	Manager	All user menu options enabled, except Installer programming Access to areas 1 to 16 Assigned to users

Table 18. Hard-coded alarm groups (continued)

Number	Name	Description
8	Spare alarm group	All user menu options disabled Cannot access any areas Assigned to devices
9	Master service	All user menu options enabled Access to areas 1 to 16 Time zone 25 assigned No alarm control Assigned to users **Note:** Alarm group 9 assigns the special soft time zone 25, reserved for service technicians. Refer to *Soft time zones* on page 233 for more details.
10	Spare alarm group	All user menu options disabled Cannot access any areas Assigned to devices

Functions

Alarm groups can be used for the following functions:

Alarm control. The ability of a user to arm/disarm the system.

Users. When adding a user to the system, the assigned alarm group will dictate the user alarm capabilities.

RAS devices. When adding a RAS device to the system, the assigned alarm group will dictate the possible alarm control capabilities supported by the device, as well as which areas the RAS can control. The RAS device also allows setting a different alarm group in order to dictate the possible menu selections.

Intelligent doors. When adding an intelligent door to the system, the assigned alarm group will dictate the possible alarm control capabilities supported by the door.

Alternate. Each alarm group allows setting an alternate alarm group in case the original is disabled due to an invalid time zone.

Programming

The following programming options are available for alarm groups:

Alarm group number

Range: 1 to 138

Specify the alarm group to program.

Note: Alarm groups 1 to 10 are hard coded. Refer to *Hard-coded alarm groups* on page 189.

Alarm group name

Range: Up to 16 characters.

Specify the name of the alarm group. The name is converted into a system text word, and is subsequently transferred to the control panel. As a result, the name will appear within RAS keypad devices.

Since the system only allows up to 100 user-defined text words, try to reuse existing text words in the text word library (see *Text word library* on page 308).

Description

Specify a 40-character text description of the alarm group. The description is not transferred to the device, and is only used by the management software.

Areas

Range: 1 to 16

Specify the areas where the alarm group will have alarm control.

Time zone

Range: 0 to 64 (includes both soft and hard time zones)

Specify the day/time the alarm group is valid.

Alternate alarm group

Range: 1 to 138

When the system is performing some functionality that depends on a valid alarm group, the control panel will resort to the alternate alarm group if the alarm group's time zone is invalid. The system will go two levels deep. For example, the system would check the validity of the primary alarm group, then its alternate alarm group, and ultimately the alternate's alternate alarm group.

Alarm group options

User alarm group	**Enabled:** The alarm group is assigned to users. **Disabled:** The alarm group is assigned to RAS devices
Alarm system control	**Enabled:** Allows arming and disarming areas assigned to the alarm group. **Disabled:** No arming or disarming is allowed. Other access control functionality defined within the alarm group is still allowed.
List of areas	**Enabled:** After a user enters a valid PIN code on an LCD keypad, all areas assigned to the user are displayed. The user can then select which areas to arm/disarm from the menu provided. **Disabled:** After a user enters a valid PIN code, the areas assigned to the user are immediately armed/disarmed once the **ON** and **OFF** keys are pressed.
Keyboard duress	**Enabled:** Allows a user to activate the duress function. This will cause a silent signal to be sent to the central station, notifying them that a user has disarmed the system while under threat. **Disabled:** Duress function is disabled for this user. The *Duress type* on page 255 must be configured in order for this function to work correctly.
Reset system alarms	**Enabled:** Allows a user to reset latching system alarms, such as DGP tamper, siren fail, and low battery. **Disabled:** Reset latching system alarms is disabled for this user.
Disable automatic unbypass	**Enabled:** During system disarm; any zones assigned to the alarm group that are in the active state are not automatically bypassed. **Disabled:** During system disarm; any zones assigned to the alarm group that are in the active state are bypassed. The *automatic unbypass when area disarmed* option in *Control panel options (see System options* on page 258*)* programming, must be enabled in order for this function to work correctly.
Arm and reset only	**Enabled:** Alarm control is restricted to only arming and reset functionality. **Disabled:** There are no alarm control restrictions. The *alarm system control* option must be enabled in order for this function to work correctly.

Disarm only	**Enabled:** Alarm control is restricted to only disarming. **Disabled:** There are no alarm control restrictions. The *alarm system control* option must be enabled in order for this function to work correctly.
Alarm reset only	**Enabled:** Alarm control is restricted to only resetting alarms. **Disabled:** There are no alarm control restrictions. The *alarm system control* option must be enabled in order for this function to work correctly.
Auto bypass active zones	**Enabled:** When arming areas begins, all zones in the active state are bypassed and the system is armed without generating any alarms. **Disabled:** The system cannot be armed if there are zones in the active state. If this option is disabled and you would like to enable forced arming, the *forced arming* option must be enabled.
Forced arming	**Enabled:** Areas assigned to the alarm group will be armed, despite any zones that might be in the active state. **Disabled:** Areas assigned to the alarm group cannot be armed as long as there are zones in the active state. When zones in the active state are forced to arm, the zone could raise an alarm. This will depend on the zone types assigned (2, 4, 28, and 68).
Prevent forced disarming	**Enabled:** Areas cannot be disarmed if there are any zones in the active state. **Disabled:** Areas can be disarmed, despite any zones being in the active state. This option is specific to zone types 1 (disarmed alarm) and 11 (disarmed delayed alarm).
Alarm group restrictions 1 to 8	**Enabled:** The corresponding alarm group restriction is activated. **Disabled:** The corresponding alarm group restriction is disabled. Only one restriction per alarm group is allowed. Enabling one restriction will disable all others.
No arming if restriction not timing	**Enabled:** An area cannot be armed if a user without an alarm group restriction disarmed it. **Disabled:** Normal alarm group restrictions apply. If an area has been disarmed and an alarm group restriction timer is not running, the alarm group restriction timer cannot be started. As soon as the alarm group restriction timer expires, the area is armed.

Change own PIN only	**Enabled:** Users can only change their own PIN codes. **Disabled:** Users can change other user's PIN codes. This will also allow users to access System Menu 14, which provides menus for deleting, displaying, and creating users. This option impacts a user's ability to create, delete, and change door groups, floor groups, and user names.

Alarm group menu options

These options dictate which system menus a user may access when using an LCD keypad. In order to access the menu, the following two conditions must be met:

- The alarm group assigned to the user must have the menu option enabled.
- The alarm group assigned to the LCD keypad must also have the menu option enabled.

The user does not have to be assigned the same alarm group as the one assigned to the keypad; they only have to have the same menu options enabled. *Table 19* shows the alarm group menu options.

Table 19. Alarm group menu options

Menu number	Menu name	Description
1	Panel status	Provides system information.
2	Active zones	Shows zones not in the normal state (active or tampered).
3	Zones in alarm	Shows any zones in alarm.
4	Bypassed zones	Shows any bypassed zones.
5	History	Lists all events in the control-panel event buffer.
6	Test report	Perform an arm/disarm test.
7	Service menu	Allows the user to request a service call or establish a connection to a remote service center in order to program the system over the telephone network.

Table 19. Alarm group menu options (continued)

Menu number	Menu name	Description
8	Film counters	Displays the current frame number position on each of the security camera films.
9	List zone names	List all known zone names.
10	Bypass zone	Bypass a zone.
11	Unbypass zone	Unbypass any zone previously bypassed.
12	Test zone	Test a specific zone.
13	Start automatic disarm test	Perform an automatic disarm test.
14	Program users	Modify user database.
15	Time and date	Modify system time and date.
16	Bypass/unbypass RAS/DGP	Bypass/unbypass any RAS/DGP device.
17	Enable/disable service tech	Enable/disable the service technician's code.
18	Reset cameras	Reset the film frame count on a camera to zero. This is done when you have changed the film in a camera.
19	Installer programming	Access installer-programming databases.
20	Door and floor groups	Modify door and floor group databases.
21	Holidays	Modify holiday database.
22	Open door	Open a door for the programmed unlock time.
23	Unlock, lock, disable, enable	Door can be unlocked until locked again with this menu. Disable or enable doors.
24	Print history	Force the system to output events to a printer.

Alarm group restrictions

Alarm group restrictions impose limits on the *Timed disarmed areas* and *Areas to arm/reset* functions for selected areas within an alarm group. Each alarm group is limited to only one restriction.

In order to support alarm group restrictions, the following criteria must be met:

- The corresponding restriction must be enabled within the alarm group itself.
- The areas defined within the restriction are also defined within the alarm group.

The one exception to the second rule is if the alarm group enables any of the following options: *disarm only*, *arm/reset only*, or *alarm reset only* in Alarm groups programming. In this case, the areas in the restriction do not need to match those defined in the alarm group.

If there are areas assigned to the alarm group, but not to the restriction, they will have standard system control functions as specified in the alarm group.

Example 1

Cleaners are only allowed to arm/reset areas 1, 2, and 3. They are not allowed to disarm any of these three areas. They can, however, disarm area 4. The implications are:

- An alarm group exists defining areas 1, 2, 3, and 4, and is assigned to the cleaners.
- This alarm group enables alarm group restriction 1, which has been configured to only allow arm/reset for areas 1, 2, and 3.

Example 2

A security guard has permission to disarm areas 3, 4, and 5. After 15 minutes, the areas rearm automatically. The implications are:

- An alarm group exists defining areas 3, 4, and 5, and is assigned to the security guard.
- This alarm group enables alarm group restriction 3, which has been configured to set areas 3, 4, and 5 for *timed disarm*.
- The *alarm group restriction disarmed time* option in *Timers* programming (see *Alarm group restriction 1 to 7 disarmed time* on page 172) is set to 15 minutes.

Functions

Alarm group restrictions can be used for the following functions:

Specify area alarm control limitations. Allows restricting alarm control to specified areas. For some areas, a user is able to arm/disarm. In others, they may only disarm.

Incorporate delays in area disarm functionality. Apply hardware timers when certain areas are disarmed.

Programming

The following programming options are available for alarm group restrictions:

Restriction number

Range: 1 to 7

Specify the alarm group restriction to program.

Name

Range: Up to 16 characters

Specify the name of the alarm group restriction. The name is converted into a system text word, and is subsequently transferred to the control panel. As a result, the name will appear within LCD RAS keypad devices.

Since the system only allows up to 100 user-defined text words, try to reuse existing text words in the text word library (see *Text word library* on page 308).

Timed disarmed areas

Range: 1 to 16

Specify the areas to program for time disarm. This includes:

- Areas that automatically rearm after a timed disarmed period
- Automatic arm/disarm areas to enable the postponed and warning time
- The timed areas required when programming vault areas

The time for the restriction is defined in the *alarm group restriction disarmed time* option in Timers programming (see *Alarm group restriction 1 to 7 disarmed time* on page 172).

Areas to arm/reset

Range: 1 to 16

Specify the areas that limit alarm control to arm/reset. This allows a user to arm areas specified by the user's alarm group or to reset alarms in those areas the user cannot disarm.

Timed disarmed areas and areas to arm/reset

When enabling areas for both functions, a user entering a code causes all the timed disarm functions to apply, except when re-entering a code, in which case, the arm/reset function applies. In the latter case, the system is armed regardless of any running timers.

Alternate alarm group restrictions

Specify additional restrictions when the original alarm group is not valid due to an invalid time zone. Each alarm group can be programmed to accept a single alternate alarm group. When the primary alarm group assigned for example, to a user is invalid due to an invalid time zone, the system will check to see if an alternate is defined. If so, the system will use the alternate. Under this scenario, the system will use the alternate alarm group restriction properties.

Table 20 shows an example of an alarm group set up.

Table 20. Alarm group example

Option	Alarm group 31	Alarm group 32	Alarm group 33
Areas	1 and 2	1 and 2	1
Alarm group restriction	4	4	4
Time zone	1	2	0
Alternate alarm group	32	33	None

Table 21 shows how the alternate alarm group restrictions are configured for the example.

Table 21. Alternate alarm group restrictions configuration

Option	Standard	First alternate	Second alternate
Timed disarm area		2	1
Arm/reset area	2		

Alarm group 31 is assigned to user 1.

When time zone 1 is valid. User 1 will have alarm group 31 with alarm group restriction 4. The user has full control over area 1 and can arm/reset area 2.

When time zone 1 is invalid, but time zone 2 is valid. User 1 will have the first alternate alarm group with alarm group restriction 4. The user has full control over area 1 and timed disarm for area 2.

When time zone 1 and time zone 2 are invalid. User 1 will have the second alternate alarm group with alarm group restriction 4. The user has timed disarm for area 1 and no control over area 2.

Automatic arm/disarm

This feature allows you to arm/disarm programmed areas at specified times. This works:

When the programmed time becomes valid, the system will disarm all areas assigned to the programmed alarm group.

When the programmed time is about to become invalid, all keypad buzzers will intermittently sound their warning buzzer. A user may postpone the arming time by either entering their PIN or badging their card during the warning time.

When the programmed time becomes invalid, the exit timer starts and all areas assigned to the programmed alarm group are armed.

Up to four off and on times may be programmed per time zone, but you cannot have a time zone disarm before midnight and rearm after midnight. If this is required, use one time zone with an end time of 24:00, and another time zone with a start time of 00:00.

Functions

Automatic arm/disarm can be used for the following functions:

Hands free arm/disarm. This feature guarantees that the system will arm/disarm at specified times, without any user interaction

Variable arm/disarm options. A number of arm/disarm options are available, based on the alarm group configuration.

Programming

The following programming options are available for automatic arm/disarm.

Program number

Range: 1 to 16

Specify the automatic arm/disarm option to program. Each combination of a time zone and an alarm group is called a program. There are 16 programs, one for each possible area. A different program must be completed for each area, or set of areas where a different function is required.

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Time zone number

Range: 0 to 24

Specify the days/times when the system automatically arms/disarms the associated areas. This option is limited to only hard time zones.

The time zone start time dictates when the areas will disarm. The time zone end time dictates when the areas will arm.

Alarm group number

Specify the alarm group to associate with the current program number. Since an alarm group defines alarm control for specified areas, this has the side effect of dictating which areas will be armed/disarmed.

The alarm group settings also determine the arm/disarm functionality. For example, if the alarm group's *arm and reset only* option in *Alarm group* programming is enabled, assigned areas will only arm. If the alarm group's *disarm only* option in *Alarm group programming* is enabled, the assigned areas will disarm.

An alarm group defines its own time zone. The assigned time zone dictates whether or not the alarm group is valid. Since this option also ties in a time zone, the assigned alarm group does not need a defined time zone. If you use an existing alarm group with a defined time zone, make sure the same time zone is used in the *Time zone number* option above.

Automatic reset

Automatic reset provides a mechanism that can automatically reset alarms after a specified period of time. When an automatic reset is configured for an alarm group, all alarms contained in the alarm group are reset after the amount of time specified has expired post alarm. The automatic reset function is useful in instances where it may not be possible to reset alarms manually.

Programming

The following programming options are available for automatic reset:

Time before alarm will reset

Range: 1 to 255 minutes

Specify the amount of time that will elapse after an alarm has been triggered and before the alarm group it belongs to automatically resets.

Alarm group to use when resetting

Range: Any valid alarm group 1 to 138

Specify the alarm group that will be automatically reset after an alarm in the group has been triggered.

Chapter 11 Diagnostics programming features

This chapter provides an overview of diagnostic programming features.

In this chapter:

Battery test

The battery test tests the state of batteries connected to system bus devices. All batteries are tested in sequence in order to prevent power problems. If a battery is disconnected for more then 10 minutes, a warning will be given. During the battery test, all of the panels and auxiliary driven devices are powered from the battery. Devices are tested one at a time to ensure that not all of the devices switch to battery test at the same time.

Programming

The following programming options are available for the battery test:

Frequency

Specify when the battery test should be conducted. The choices include:

Disabled. The battery test is not conducted.

Every working day. The battery test is conducted each day.

Every Monday. The battery test is conducted each Monday.

First Monday of the month. The battery test is conducted on the first Monday of each month.

Start time

Specify the time of day, in hours and minutes, when the battery test will start.

Run time

Range: 2 to 255 (minutes)

Specify the time period that the battery test will run.

Test on holiday

If enabled, the battery test will be conducted on holidays. This implies that the test will likely occur outside the bounds of the specified frequency.

Clock correction

This option allows you to program a correction factor that compensates for a control panel clock that may be running slightly fast or slow.

Programming

The following programming options are available for the clock correction feature:

Clock correction

Range: 119 to 199 seconds per day

Specify the amount of time to compensate a control panel per day.

Daylight savings start month

Range: January through December

Specify the month that daylight savings time begins.

Daylight savings end month

Range: January through December

Specify the month that daylight savings time ends.

Start daylight savings

Range: See daylight savings start/end table.

Specifies the Sunday of the month when daylight savings time begins.

End daylight savings

Range: See daylight savings start/end table.

Specify the Sunday of the month when daylight savings time ends.

Daylight savings start/end table

Table describes the daylight savings time start/end choices.

Table 22. Daylight savings start/end

Option	Description
Disable	No daylight savings time setting required.
First Sunday	Daylight savings time starts/ends on the first Sunday of the specified month.
Second Sunday	Daylight savings time starts/ends on the second Sunday of the specified month.
Third Sunday	Daylight savings time starts/ends on the third Sunday of the specified month.
Fourth Sunday	Daylight savings time starts/ends on the fourth Sunday of the specified month.
Last Sunday	Daylight savings time starts/ends on the last Sunday of the specified month.

Next service

This option allows you to set a date for programmed text to display on the LCD arming station indicating that the next routine service call is due.

Programming

The following programming options are available for the nest service feature:

Next service date

Specify the date on which the next routine, service call is due.

Next service text

Specify the 32 characters of customized text that will be displayed on the LCD arming station for the programmed next service date.

This option will be used to remind end-users when the next routine service call is due and can also be used for those end-users who have opted not to have a service/ maintenance contract.

The control panel can be armed, disarmed, or controlled normally by the end-user. However, the programmed service text will continue to appear on the display of the RAS device until the engineer has entered the Engineer menu.

Test call

Test call performs a regular interval report call to the central station. This allows the system to ensure that central station reporting is working and that no problems have occurred that would prevent it from reporting access and alarm events. All tests are reported as a test call to the central station.

Types

The following types of test calls are available:

No test. No automatic test calls made, test calls must be activated manually.

Enable automatic test. The disarm or arm test starts automatically when the system is disarmed or armed.

Manual disarm test/automatic arm test. The arm test starts automatically when the system is armed. The disarm test can only be done using user menu 13 on the LCD keypad, *Start Auto Disarm Test*.

Automatic disarm test only. The disarm test starts automatically when the system is disarmed. No arm test is available.

Programming

The following programming options are available for the test call feature:

Start test call at

Range: 24-hour time format (hh:mm)

Specify the time the test call should be made. The time programmed is based on the control panel's real time clock.

Test call interval

Range: 2 digits (hours)

Specify the interval between test calls.

Extend test call

If enabled, the test call will be performed only if no events have been reported to central station 1 during the text call interval; otherwise, the test call will be performed as specified regardless of events reported to the central station.

Chapter 12 Reporting programming features

This chapter provides an overview of reporting programming features.

In this chapter:

Central Station

The system supports up to four different central stations, each allowing a variety of different formats. When certain events take place, the central station configuration is used to determine if the events are reported and what format will be used.

Programming

The following programming options are available for the central station:

Central station number

Range: 1 to 4

Specify the central station to program.

Description

Specify a 40-character text description. The description is only used by the management software.

First phone number

Specify the main central station phone number.

Second phone number

Specify the backup central station phone number.

System account number

Range: 4 to 6 digits (enter *0000* if system event reporting is not required)

Specify the alarm system reporting to the central station. The account number is used to identify system events not linked to an area.

Area account number 1 to 16

Range: 4 to 6 digits (enter *0000* if system event reporting is not required)

Specify the area account number for a specific system area. Area account number 1 handles area 1; area account number 2 handles area 2, etc.

Do not program more account numbers than there are areas in the system. For example, a system consisting of only Area 1 and 2 should program the two area account numbers, plus the system account number (if required).

For SIA/XSIA reporting, programming the same area account code for different areas within 1 central station will result in common area reporting: the first area with that account code that disarms will send an opening. The last to close will send the closing.

Format

Define the central-station reporting format.

0 = Disabled

1 = Tecom Dialer V1 (only used in Australia)

2 = Contact ID - Small

3 = Contact ID - Large

4 = SIA - Small

5 = SIA - Large

6 = XSIA - Small

7 = XSIA - Large

8 = 200 baud FSK Format 1

9 = 200 baud FSK Format 2

10 = 200 baud FSK Format 3

11 = 200 baud FSK Format 4

12 = X25 Enai

13 = Voice Reporting - Acknowledge

14 = Voice Reporting - No Acknowledge

18 = Securitel Serial

19 = Securitel PIN

Securitel is a direct line format. This implies that the panel will not report other programmed CSXs, or answer incoming calls to the on-board modem unless there's an error. Only one central station can be programmed to Securitel.

If X25 Enai format is selected, the panel will automatically assume that the connection type is ISDN-D channel.

The difference between *Small reporting* and *Large reporting* is the amount of system events that will be reported. The *Large* formats will report most system events, while the *Small* formats will report summarized events.

Connection type

Define what physical medium is used to call the central station. Options include:

PSTN. Uses the on board dialer to make the call

ISDN. Uses the AL-7100 plug-in dialer device to make call

GSM. Hardware is not yet available

Use Bell 103 protocol

Enable to use the Bell 103 modem tones for the PSTN/ISDN analog line connection.

Dual reporting

If enabled**,** an acknowledgement should be received from both central station telephone numbers. If disabled, the first acknowledgement received will close down the dialer, unless there are more reports pending (commonly referred to as alternate reporting).

Disable reporting bypasses

If enabled, bypasses are not reported. If disabled, they will be reported.

XSIA max characters: 16 (off) 30 (on)

Enable to specify the maximum number of XSIA characters is 30; otherwise, the maximum is 16.

Suppress FTC for voice reporting

Enable to suppress the Report Fail (FTC) message and fault LED on the RAS. This option is only applicable if voice reporting is the selected protocol.

X25 account code

Range: 8 digits maximum

Specify the account code for X25 protocols.

X25 line type

Set the polling time of the line from one of the following options:

0. Permanent 15 minutes polling

1. Permanent 90 seconds polling

Communication programming

Communication programming establishes all system wide central station communication options. The settings programmed here are used in conjunction with the central station reporting setup.

PABX number

Range: 18 digits maximum

A PABX (private automatic branch exchange) number includes a number that precedes the phone number in order to connect to an outside line. This should only be used if the dialer is connected via a PABX to the telephone network. In most cases, either 9 or 0 is used to access an outside line.

MSN number

Range: 17 digits maximum (may not contain the characters P and T, but only digits between 0 and 9)

Specify the number used for an ISDN dialer. The number is sent to the ISDN network when dialing out to the central station. This number is also used for remote programming when dialing in.

Dial-tone detection

Specify the appropriate dial tone. If dial tone detection is not disabled, dial tone detection will occur at the beginning of the dialing process, after dialing the PABX number, or when an '*' (asterisk) character is identified in the dialed number. Dial tone options are shown in *Table 23*.

Table 23. Dial tone options

Dial tone	Description
0	Disabled
1	CTR21
2	Netherlands
3	UK
4	Other

X25 TEI value

Range: 1 to 63

Specify the value given by the telecom for the ISDN connection.

Audio listen-in time

Range: 10 to 255 (seconds)

Specify the total audio time transmitted.

Audio listen-in frame time

Range: 30 to (Audio listen-in time) (seconds)

Specify the frame interval that the audio is transmitted. Audio listen-in time option dictates maximum range.

Central station communications options

Tone dialing	**Enabled:** Use tone dialing for PSTN telephone lines. **Disabled:** Use pulse dialing for PSTN telephone lines. This option is not used for ISDN connections.
Enabled line fault monitor	**Enabled:** The system will detect if the line voltage on the telephone network is within limits. If not, a telephone line fault condition will be activated. **Disabled:** Line fault monitoring is disabled. This option should only be used for PSTN connections.
3-digit SIA extensions	**Enabled:** SIA and XSIA reporting uses 3-digit numbers. **Disabled:** SIA and XSIA reporting uses 2-digit numbers. When 2-digit numbers are used, any number above 99 (3-digit numbers) will be converted to 99.
ISDN point-to-point	**Enabled:** ISDN point-to-point enabled. **Disabled:** ISDN point-to-multipoint enabled. This option should only be used for ISDN connections.
Enable ISDN line\fault monitor	**Enabled:** The system will detect if the line voltage on the ISDN network is within limits. If not, a telephone line fault condition will be activated. **Disabled:** Line fault monitoring is disabled. This option should only be used for ISDN connections.
200 Baud reverse area armed/ disarmed	**Enabled:** Disarm events are reported as type R and arm events are reported as type A. **Disabled:** Disarm events are reported as type A and arm events are reported as type R.
Report AC fault	**Enabled:** Should be enabled for all countries except Ireland. **Disabled:** By default for Ireland. This option is ignored if the *enable buzzer on AC/line fault* option is enabled in *Control panel options* programming (see *System options* on page 258).

Report line fault	**Enabled:** Should be enabled for all countries except Ireland. **Disabled:** By default for Ireland. This option is ignored if the *enable buzzer on AC/line fault* option is enabled in *Control panel options* programming (see *System options* on page 258).
Enable GSM line fault monitoring	Hardware is not yet available for this option.
SIA area modifier	**Enabled:** The area modifier code packet will be added to the SIA transmission. This allows the user to send to multiple areas using the same amount of code. **Disabled:** The area modifier code packet will not be added to the SIA transmission.

Reporting classes

Reporting classes let you specify what is reported in the event of an alarm. When a zone triggers an alarm the assigned reporting class is reported to the configured central stations.

Programming

The following programming options are available for reporting classes:

Reporting class

Range: 1 to 8

Select the reporting class that you would like to program. *Table 24*details the reporting classes.

Table 24. Reporting classes

Reporting class	Name
1	Medical
2	Emergency alarms
3	Panic alarms
4	Burglar alarms
5	General alarms
6	24-Hour alarm
7	Emergency supervisory
8	System alarms

Reporting condition

Range: 1 to 6

Select the condition to program. Every class can report 6 conditions detailed in *Table 25*.

Table 25. Reporting conditions

Reporting condition	Name
1	Alarms
2	Alarms restore
3	Tamper
4	Tamper restore
5	Bypass
6	Bypass restore (unbypass)

Report to central station

Range: 1 to 4

Specify the central stations this reporting class will report to when the designated reporting condition is triggered.

Enable audio listen-in

Enable audio listen-in for the reporting class condition specified.

Voice reporting

Voice reporting works in conjunction with a voice communications module to send voice reports to a specified phone number.

Programming

The following programming options are available for voice reporting:

Event number

Range: 1 to 25

Specify the event to associate this voice report with. Each voice report can be programmed using either a standard event number (1 to 11) or an event number that exists in the user defined event tables (12 to 25) as shown in *Table 26*. Using an event from the user tables (12 to 25) allows for greater flexibility as macros can then be used to trigger these event codes from various sources.

Note that event code 12, 130 BA Burglary, and event code 1, Burglar Alarm, are the same event code (130). If event code 12, 130 BA Burglary, is programmed with an alarm message, it will have priority over event code 1, Burglar Alarm.

Table 26. Event numbers

Event number	Name
1	Burglar Alarm
2	Tamper Alarm
3	Hold-up Alarm
4	Panic Alarm
5	Emergency Alarm
6	Medical Alarm
7	Technical Alarm
8	AC Fail
9	DGP Offline

Table 26. Event numbers (continued)

Event number	Name
10	Area Armed
11	Area Disarmed
12	130 BA Burglary
13	131 BA Perimeter
14	132 BA Interior
15	133 BA 24-Hour
16	134 BA Entry/Exit
17	135 BA Day/Night
18	136 BA Outdoor
19	137 BA Tamper
20	138 BA Near Alarm
21	140 UA General Alarm
22	YT Battery Low
23	YR Battery Restore
24	AR AC Restore
25	ZR Technical Restore

Voice message number

Range: 0 to 14

Specify the voice message that has been programmed on the AL-7200 communications module to be used with this voice report. The value of 0 (zero) specifies that no voice message should be used.

Description

Add comments about the specified voice report. This information is not downloaded to the control panel.

Chapter 13 Time and date programming features

This chapter provides an overview of time and date programming features.

Hard time zones

Hard time zones define periods of time, including the time of day and the day of the week. They are typically used to allow or prevent certain actions from taking place.

The control panel provides 25 hard time zones. The first time zone (Time Zone 0) is hard-wired to 24-hours and cannot be changed. The other hard time zones contain four sub-time zones allowing different start/end times, as well as days of the week. In addition, each sub-time zone allows inclusion of holidays above and beyond the times/dates specified. A time zone is considered active as long as one of the four sub-time zones is valid. If holidays are enabled for the time zone, then it is possible for all four sub-time zones to be invalid, but the overall time zone to be active due to the current day falling on one of the defined holidays.

Functions

Hard time zones can be used for the following functions:

Door group. Dictates the times a user assigned to a door group can access RAS devices on the system bus, as well as intelligent doors found on the 4-Door Controller.

Alarm group. Dictates the times a user assigned to an alarm group can control (arm/disarm) specified areas.

Floor group. Dictates the times a user assigned to a floor group can access programmed floors.

Relay. Dictates the times a relay may be activated when mapped to an event flag.

Macro logic. Because macros inherently use event flags as input, time zones dictate the times when macros are functional.

Programming

The following programming options are available for hard time zones:

Time zone number

Range: 1 to 24. Time zone 0 defaults to 24-hours.

Specify which hard time zone is being programmed.

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Start time

Specify the start time for the time zone, in hours and minutes.

End time

Specify the end time for the time zone, in hours and minutes.

Days of the week

Specify the days of the week the time zone will be active.

Include holidays

If enabled, the time zone will be valid for all days defined by the system holidays.

Holidays

Holidays are used in conjunction with time zones in order to define additional access parameters. Under many programming options, a given function will only take place when the assigned time zone is valid/invalid. When the holiday becomes valid, regardless of the days programmed within the time zone, the overall time zone state becomes valid.

Functions

Holidays can be used for the following functions:

Additional time zone parameter. Provides an additional access parameter to the time zone. If a time zone would normally be invalid, a holiday could cause it to become valid if the current day matches the holiday.

Additional access parameter. A user is normally denied access to a door when all existing time zones are invalid. If the holiday is valid, however, access will be granted.

Programming

The following programming options are available for holidays:

Holiday number

Range: 1 to 64

Specify which time zone is being programmed.

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Date

Specify the date given to the holiday.

Chapter 14 Zone and relay programming features

This chapter provides an overview of zone and relay programming features.

In this chapter:

Relays

A relay can have one of the following forms:

Physical. A physical relay can be found on some of the control boards, as well as relay expander boards. Each physical relay is numbered based on the device bus address of the parent device. See *Numbering* on page 324.

Logical. A relay can be used within the system for logical purposes, without any associated physical relay. For example, an event flag is raised due to a system macro, which then causes the logical relay to go active. This logical relay may then be used in soft time zone programming. In this case, there is no physical relay involved in the process. In fact, the relay can be viewed as a variable that is assigned a true/false logic value.

Either a time zone or an event flag will drive the relay state. In the case of event flags, some relay numbers have associated hard-wired event flags.

Relay numbers hard-wired to event flags

Table 27 lists the relay numbers hard-wired to event flags.:

Table 27. Relays hard-wired to event flags

Relay number	Event flag
2	Event flag 2 (strobe)
3	Event flag 1 (external siren)
12	Constant DC voltage at the siren output
13	A warble tone at the siren output
14	A saw-tooth tone at the siren output
15	Two tones at the siren output
	Event flag 13 (internal siren)
16	An inverted sawtooth tone at the siren output
	Event flat 1 (control panel external siren)
32,48,64,80,96...240	Event flag 1 (DGP external siren)

Functions

Relays can be used for the following functions:

Event flag. Associate the relay with an event flag. When the event flag is raised, fire the relay.

Time zone. Associate the relay with a time zone. The time zone state will drive the relay.

System macro. Relays are used as inputs in constructing the macro equation.

Siren tones. Hard-wired relays are used to produce different siren tones.

Programming

The following programming options are available for relays:

Relay number

Range: 1 to 255. (See *Numbering* on page 324)

Specify which relay is being programmed.

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Activated by event flag

Range: 1 to 255

Specify the event flag which, when raised, will cause the relay to become active. This option assumes the time zone is not valid. If the time zone is valid, then the time zone state will drive the relay.

Inactive during time zone

When the time zone is valid, the relay is never activated. When the time zone is invalid, the event flag will drive the relay.

Time zone

Range: 0 to 64

Specify the time zone when the relay can be active or inactive. When a time zone is valid and assigned to a relay, the relay state is completely driven by the time zone state, regardless of the event flag state. When the time zone becomes invalid, the relay is then driven by the event flag state.

Output inverted

If enabled, the overall logical result is reversed. The relay is inactive when this option is set if, based on all programmed options, the relay would normally be active.

Set output text

Specify the text message that is displayed by the management software when the relay state is set.

Reset output text

Specify the text message that is displayed by the management software when the relay is reset.

Soft time zones

The control panel provides 16 programmable soft time zones. Soft time zones, are similar to system macros in that they are programmable logic that can ultimately be used to enable/disable certain actions. Soft time zones are also used to program keypad function keys (F1-F4). Soft time zones are only active when the associated relay is active. The state of the relay will drive the state of the time zone. A special soft time zone is provided that can prevent service technicians from accessing the control panel.

Functions

Soft time zones can be used for the following functions:

Door group. Dictates whether or not a door can be opened when a soft time zone is assigned to the door group.

Relay. A soft time zone is only valid when the relay that is associated with the time zone is active; otherwise, it is invalid.

Types

Alliance provides the following types of soft time zones:

Service technician. Soft time zone 25 is hard-wired and cannot be programmed. This time zone is used to grant/deny access to the service technician.

Programmable. Soft time zones 26 to 41 are standard soft time zones.

RAS function keys. Soft time zones 42 to 63 are assigned to specific RAS function keys.

Programming

The following programming options are available for soft time zones:

Soft time zone number

Range: 26 to 41

Specify which time zone is being programmed.

Description

Specify a 40-character text description. The description is not transferred to the device, and is only used by the management software.

Output to follow

Specify the relay (output) assigned to the time zone. The time zone validity follows the relay state. For example, the time zone is active when the assigned relay is active and is inactive when the assigned relay is inactive.

Service technician setup

The system provides soft time zone 25. This time zone is hard-wired and cannot be programmed. It is used in alarm group 9 to grant access to an installer servicing the system. The state of the time zone is only active when Service technician (menu 17) is enabled.

Function key programming

In order to program the keypad function keys, the RAS device address must be between 0 and 4. Also, the relay you want to become active when a function key is pressed must have the associated soft time zone programmed.

Example. To activate relay 100 when F1 is pressed on RAS number 1:

- Create relay 100.
- Based on the table x, soft time zone 42 must be used. In the *time zone* option in *Relay programming* (see *Time zone* on page 232), assign time zone 42.

Function keys

Table details the function keys.

Table 28. Function keys

Function key	Soft time zone range
RAS 1 function keys (F1-F4)	42 to 45
RAS 2 function keys (F1-F4)	46 to 49
RAS 3 function keys (F1-F4)	50 to 53
RAS 4 function keys (F1-F4)	54 to 57
RAS 5 function keys (F1-F4)	58 to 61
RAS 1 to 16: F1 function key pressed more than 2 seconds.	62
RAS 1 to 16: F2-F4 function keys pressed more than 2 seconds.	63

Zones

A zone, also known as an input, is typically a sensor wired either directly into the control panel, through a DGP, or through an expander board. When the zone is in its active state, a signal is passed to the control panel and depending on a variety of conditions, further action may be taken. Typical sensors include:

- Motion sensors
- Glassbreak sensors
- Buttons (such as push buttons or RTE buttons)

Within the system, zones can also be used in conjunction with event flags in order to establish logical states. Each zone is programmed to accept an event flag that is raised whenever the zone becomes active. For example, system macros are based on creating logical equations from a series of event flags. When one or more event flags are active (in a logical true state), the system will perform some other function.

In general, the control panel will constantly monitor zones for changes in state in order to execute some other action. In some cases this will include notifying the central station that an alarm has occurred.

Zones are assigned to either alarm groups or areas, but not both. The zone type will determine which is required. An alarm group is assigned for zone types 6, 31, 34, and 35. These zones are typically used for keyswitches to arm and disarm areas. The affected areas will come from the assigned alarm group definition.

All other zone types are assigned areas so that alarm information can be sent to the respective areas and central station. Also, in assigning areas to zones, the alarm can be reset when the alarm occurs. In general, zones are assigned specific areas in order to dictate which areas will be in alarm when the zone becomes active.

The control panel uses the zone type to determine how to treat the zone when an assigned area is armed or disarmed. The system supports seventy different zone types, as shown in *Zone types* on page 344 and it is important to clearly understand the ramifications in choosing one type over another such as:

Armed zone types. The system will only generate an alarm if the associated area is armed.

Disarmed zone types. The system will only generate an alarm if the associated area is disarmed.

Entry/exit zone types. Areas define the entry/exit times, therefore, the system will use the longest time associated with the zone. For example, if an entry/exit zone is assigned to areas 1 through 3 and the zone is in alarm, the system will use the longest entry/exit time defined within those three areas.

Event flags and zones are closely linked. When a zone goes into alarm, the assigned zone event flag is raised. This event flag may be used in a variety of ways, depending on the required functionality. A typical use is to associate the event flag with a relay. When the zone goes into alarm, the event flag is raised and trips the relay.

Each zone provides numerous system-wide event flags that can be raised during an alarm. These include:

- Internal/external siren
- Keypad buzzer
- Armed/disarmed alarm

Text words are used in defining the zone name. Unlike numerous other program elements, zone name text words are downloaded to the panel. LCD keypads will use these text words when displaying the zone names. When used effectively, this makes it very easy to identify zones from keypads or through management software.

Functions

Zones can be used for the following functions:

Central station. Zones can be configured to notify programmed central stations during alarm condition.

Event flags. When a zone goes into alarm, the assigned zone event flag is raised, along with numerous other system-level event flags.

Relays. Along with the event flags, zones can be programmed so that the state will cause physical relays to activate.

Area alarm control. Zones can be configured to arm/disarm assigned areas by authorized users.

Macros. Macros can accept event flags as inputs within the logic equation. Any of these inputs can correspond with zone event flags.

Programming

The following programming options are available for zones.

Zone number

Range: 1 to 256

Specify which zone is being programmed.

Zone name

Range: Up to four text words and/or four numbers.

Specify the name of the zone. The name is converted into text words, and is subsequently transferred to the control panel. As a result, the name will display in LCD RAS keypad devices.

Each zone name conforms to the following scheme, where *TW* represents a text word, and *number* represents an optional numeric value between 1 and 255.

TW1 + number 1 + TW2 + number 2 + TW3 + number 3 + TW4 + number 4

Under this scheme, it is possible to have up to four text words and four numbers. When dealing with text words, use single quotes when delimiting multi-word text words.

Example. ‘Front Main Door’ 21 ‘First Floor’

In this case, the system will view the first series of characters as a single multi-word text word. When the system displays the full zone name, it would appear as:

“Front Main Door 21 First Floor”

Care should be taken when single-quoting unique text. The system only provides 100 custom user-defined text words. Reuse as many of the predefined text words in the text word library as possible, to ensure that you do not run out of text word resources.

The numeric field that separates each of the four text words is optional. If a number exists between text words and exceeds 255, the system will view this as a text word.

Zone type

Range: 0 to 70

Specify the behavior associated with the zone when the system is armed or disarmed. See *Zone types* on page 344.

Areas

Range: 1 to 16

Specify which areas are assigned to the zone. When the zone goes into alarm, the assigned areas are notified and will dictate what the system should do with the alarm condition (i.e. report the alarm to the central station). The ability to program areas is determined by zone type. Either areas or alarm groups can be assigned zones, but not both.

Alarm group

Range: 1 to 138

Specify the assigned alarm group. The primary use is to arm/disarm areas for limited zone types. The ability to program alarm groups is determined by zone type. Only zone types 6 (pulsed keyswitch), 31 (latching keyswitch), 34 (area disarmed/alarm group restriction armed), and 35 (area alarm group restriction armed only) allow you to specify the alarm group.

Either areas or alarm groups can be assigned zones, but not both.

Zone event

Range: 0 to 255

Specify the event flag that is raised when the zone becomes active. Some event flags will be active 24 hours a day, others when armed or disarmed. The zone type will determine these circumstances, and consequently, whether or not a zone is active.

Reporting code

Specify the alarm to be reported when the zone generates an alarm. The reported event is taken from *Reporting class* programming (see *Reporting classes* on page 221). The actual message that is reported to the central station depends on the selected protocol and the selected class and sub-class. The class holds the basic reporting range (i.e. medical, panic), while the sub-class is used to provide further differentiation for the event being reported.

Test option

Purpose: Specify the zone testing procedure during arm/disarm test. In order to enable zone testing, the *test mode* option in *Control panel options programming* (see *Test mode* on page 253) must be configured. *Table 29*details the test types.

Table 29. Test types

Test type	Description
No testing required	The zone is not testing during an arm/disarm test. The zone is disabled during the disarmed test.
Test during disarm	The zone is tested during a disarm test. The zone is disabled during the test.
Tested in arm test and disarmed	The zone is tested during both the arm/disarm test.
Test during arm test	The zone is tested during the arm test.
Set event flag 13 during disarm test (internal siren)	The zone is tested during the disarm test, and event flag 13 is raised. This test is intended for testing devices activated by disarmed alarm zones, such as panic alarm buttons.
Set pre-alarm during disarm test	The zone is tested during the arm test and will raise the *pre-alarm event flag* defined in *Area programming*. This test is intended for devices that are activated during the delayed panic alarm button time.
Frequently used detector	Indicates this zone will be used during remote diagnostics in order to determine which zone has not been triggered during the last six hours after the last arming.

Enable soak test

Purpose: Enable the zone soak test mode. The soak test period is started when this option is enabled. This period of time, from 0 to 255 days, is set in *soak test days* in *Control panel options programming* (see *Soak test days* on page 257). If the value is set to zero, the soak test period is infinite and must be disabled by the user. The test results are logged in the history file.

The soak test can be used to diagnose problems without causing false alarms. When a zone is set to soak test, it **does not**:

- Report to central station
- Activate siren
- Activate strobe
- Activate any outputs (relays)

The change of the zone state is logged in the history file with events soak alarm and soak alarm restore. If the zone does not go into alarm during the soak test period, the enable soak test option for that zone will be reset when the soak test period has elapsed. If the zone goes into alarm during the soak test period, the soak test period is extended by the amount of time specified in soak test days.

Engineer walk test

Allow an engineering walk test to be conducted by a service technician.The engineer walk test is done when areas are not armed so that alarms do not report to the central station or activate relays. During this test, each zone’s frequently-used status will be updated as in normal access mode.

Double knock

Configure a zone for double knock activation in a certain time interval. If this option is enabled and a zone becomes active, at the point where the alarm condition will normally be activated, two zone timers will be triggered. An interval timer is preset (with the value programmed in *Double-knock interval* on page 175) and begins counting down. A duration timer is also preset (with the value contained in *Double-knock duration* on page 176), and counts down.

Only the following zone types can use the double knock option:

Type 1. Disarmed alarm

Type 2. Armed alarm

Type 4. Access alarm

Type 14. Access alarm (no arm check)

Event flags

External siren	**Enabled:** The *external siren event flag*, specified in *Area programming*, is activated during an alarm, and all areas assigned to the zone are armed. **Disabled:** The external siren event flag is not activated by an alarm.
Keypad buzzer	**Enabled:** When the zone is in alarm, the RAS device buzzers are activated. The system will determine which RAS devices should be buzzed based on the assigned areas defined for the zone. The system will then go through each RAS device, determining the assigned areas through the programmed alarm group. Any RAS device whose area list matches the zone area will be buzzed. **Disabled:** The RAS device buzzers are not activated during an alarm.
Make all events 24 hour	**Enabled:** All armed/disarmed event flags are raised when the zone is in alarm, regardless of area status. **Disabled:** The armed/disarmed event flags are raised strictly based on the status of the assigned areas.
Trigger armed alarm event flag 2, 3, 4, 5, 9, 11	**Enabled:** Event flag 2 is raised when the zone is in alarm and the area is armed. **Disabled:** Event flag 2 is not raised when the zone is in alarm.
Trigger disarmed alarm event flag 6, 7, 13	**Enabled:** Event flag 6 is raised when the zone is in alarm and the area is disarmed. **Disabled:** Event flag 6 is not raised when the zone is in alarm.
Trigger event flag 8, 24-hour	**Enabled:** Event flag 8 is raised when the zone is in alarm regardless of the area status. **Disabled:** Event flag 8 is not raised when the zone is in alarm.
Internal siren event flag	**Enabled:** The internal siren event flag is raised when the zone is in alarm. **Disabled** The internal siren event flag is not raised when the zone is in alarm. The *internal siren event flag* is programmed in *Area programming* (see *Event flags* on page 182) for each of the areas assigned to the zone.
Trigger zone event flag when active	**Enabled:** The zone event flag is raised when the zone is active, regardless of the status of the areas assigned to the Zone. **Disabled:** The zone event flag is only raised when the zone is in alarm (i.e. the zone is active and the area is armed).

Trigger camera event	**Enabled:** The camera event flag is raised whenever the zone is in alarm and the area is disarmed. **Disabled:** The camera event flag is not raised. You must program the *camera event flag number* option in *Area programming* (see *Event flags* on page 182) for each of the areas having cameras assigned to the zone. To activate the camera event flag when the area is armed, enable the *make all events 24 hour* option. When this option is enabled, the *internal siren event flag* option is ignored.
Print zone when active	**Enabled:** When the zone is active, a report is generated to the printer, as well as the management software. **Disabled:** A report is not generated to either the printer or the management software when the zone is active.

Reporting

Report alarm to central station 1, 2,3, and 4	**Enabled:** When the zone is in alarm, a report will be sent to the specified central station. **Disabled:** No report is sent to the specified central station. The selected central station corresponds to *Central station programming*. For example, enabling central station 1 would result in the system sending a report to central station number 1.
Enable engineer reset for alarms	**Enabled:** Engineer reset is enabled for all alarms in this zone. For example, when enabled, the user cannot arm the areas belonging to the zone until an engineer reset has been performed. **Disabled:** No engineer reset. **Note:** An engineer reset may be performed through programming menu 51 on an LCD keypad.
Enable engineer reset for tamper alarms	**Enabled:** Engineer reset is enabled for tamper alarms in this zone. For example, when enabled, the user cannot arm the areas belonging to the zone until an engineer reset has been performed. **Disabled:** No engineer reset. **Note:** An engineer reset may be performed through programming menu 51 on an LCD keypad.
Disable bypass	**Enabled:** A user cannot bypass this zone. **Disabled:** A user can bypass this zone.

Zone channel

Not Supported

Zone shunts

A zone shunt will bypass a zone for a specified period of time when the zone is in the active state. When a zone associated with a zone shunt becomes active or when the programmed output is active, a timer is started. As long as the timer is running, the zone will not cause an alarm to be generated. During this time frame, a warning timer can also be specified that could be applied to indicate that the zone is about to become active. As soon as the shunt timer expires, the zone will generate an alarm if it is in the active state.

Functions

Zone shunts can be used for the following functions:

Doors. When an unlock relay is initiated, you can bypass certain zones for a specific period of time.

Alarms prevention. Prevents zones that become active from generating alarms for a specified period of time.

Warnings. Can be programmed to give warning that the zone shunt is about to expire.

Output to start timer. An optional output can be used to start the shunt timer.

Shunt event flag. Raises a shunt event flag that can be used by other programming mechanisms. For example, when a zone is shunted, trigger a relay in order to perform some other function.

Shunt behavior. Provides several options that dictate the behavior of the zone shunt.

Programming

The following programming options are available for zone shunts:

Shunt number

Range: 1 to 16

Specify which zone shunt is being programmed.

Description

Specify a 40-character text description of the zone shunt. The description is not transferred to the device, and is only used by the management software.

Zone number to shunt

Range: 0 to 255

Specify the zone number to be shunted for the programmed time.

Shunt warning time

Range: 0 to 255 (seconds)

Specify the period of time prior to the shunt timer expiring that the shunt warning event flag should be raised.

Relay number

Range: 0 to 255

Specify the relay to start the shunt timer. If the relay is always active, the zone will always be shunted. As soon as the relay deactivates, the shunt timer will begin. When a relay is used, the total shunt time is the time the relay remains in the active state plus the shunt time.

Shunt event number

Range: 0 to 255

Specify the event flag that is raised during the shunt time period.

Shunt time

Range: 0 to 254 (refer to table)

Specify the period of time in which the zone will be shunted. While the timer is running, a zone in the active state will not generate an alarm. *Table 30* shows the shunt time ranges.

Table 30. Shunt time ranges

Shunt time range	Description
1-127	Time period in seconds.
128 + number of minutes	Time period in minutes. Under this condition, add 128 to the total of the number of minutes.

When programming one to two minute periods, set the time in seconds. Do not use a time of 0 seconds for doors if *cancel door event* is disabled. This could cause the zone to be shunted indefinitely.

Shunt warning event number

Range: 0 to 255

Specify the event flag that is raised when the shunt warning timer is active.

Zone shunt options

Door open command	**Enabled:** A RAS keypad OUT relay is used to start the shunt timer, or a shunt output is used to start the shunt timer. The shunt timer resets if the zone does not switch to the active state within: • Three seconds if the shunt time is programmed for 1 to 127 seconds • Three minutes if the shunt time is programmed for 1 to 127 minutes. If this option is enabled, entry/exit shunt must be disabled. **Disabled:** The programmed zone state starts the shunt timer.
Zones holds event	**Enabled:** A 2-second delay is applied after the zone switches to the normal state, and before it cancels the door event flag and shunt timer. **Disabled:** There is no delay.
Shunt when disarmed	**Enabled:** The assigned zone will be shunted when the areas associated with the zone are disarmed. **Disabled:** The assigned zone will not be shunted when the areas associated with the zone are disarmed.
Entry/exit shunt	**Enabled:** The assigned zone is treated as an entry/exit zone. A code must be entered to start the shunt timer; otherwise, an alarm is generated. If this option is enabled, *door open command* must be disabled. **Disabled:** The assigned zone is not treated as an entry/exit zone.
Shunt when armed	**Enabled:** The assigned zone will be shunted when the areas associated with the zone are armed. **Disabled:** The assigned zone will not be shunted when the areas associated with the zone are armed.
Log door open/close	**Enabled:** The assigned zone will be logged to the printer as *door open* or *door closed* when the zone becomes active. If *print zone when active* in *Zone programming* (see *Event flags* on page 243) is enabled for the assigned zone, a door open message is sent twice. **Disabled:** No reporting is logged to the printer.
Cancel door event	**Enabled:** When the assigned zone switches to the deactivated state, the door unlock event and the shunt timer are cancelled. **Disabled:** When the assigned zone switches to the deactivated state, the door unlock event and the shunt timer will continue to run for the programmed time.

Chapter 15 Miscellaneous programming features

This chapter provides an overview of miscellaneous programming features.

Control panel options

System options are a collection of options that affect various functions in the system. Due to the global nature of system options, any system option that is set will affect all related functionality in the system.

For example, if the *bypass zone tamper* option is enabled, all zone tamper alarms in the entire system will be bypassed.

Programming

The following programming is available for the control panel options:

Areas for total disarm

Areas specified for total disarm will bypass all of their zones when disarmed, including zones that are not disarmed normally such as 24-hour zones. Tamper alarms still function for all zones, regardless of whether or not the zone is included in an area specified for total disarm.

For example, Zone 6, a motion sensor in a room, is programmed as a 24-hour zone type and is assigned to areas 1 and 16. Area 16 is programmed for total disarm in system options.

When servicing the room where the sensor is located, area 16 will be disarmed. Zone 6 will be disarmed because it is a part of area 16.

Table 31 shows the state of zone 6 in response to the arm and disarm states of the areas it belongs to in the example above.

Table 31. Zone behavior for example

Area 1 state	Area 16 state	Zone 6 behavior (24-hour zone)
Armed	Armed	Normal operation.
Disarmed	Armed	Normal operation.
Armed	Disarmed	Zone disabled (except for tamper.)
Disarmed	Disarmed	Zone disabled (except for tamper.)

Film low

Range: 0 to 9999

Specify the film low frame count for the system. When the film frame count for system still video or still photo cameras is reached, the system will report a film low warning to the central station.

Film out

Range: 0 to - 9999

Specify the film out frame count. When the film out frame count for system still video or still photo cameras is reached, the system will report a film out warning to the central station.

Test mode

Specify the test call mode for the system. The type of test call selected determines the system tests that will be performed and at what interval they will take place. *Table 32* describes the test call types.

Table 32. Test call types

Test call type	Description
No test	No automatic test calls made, test calls must be activated manually.
Enable automatic test	The disarm or arm test starts automatically when the system is disarmed or armed.
Manual disarm test/ automatic arm test	The arm test starts automatically when the system is armed. The disarm test can only be done using user menu 13 on the LCD keypad, Start Automatic disarm Test.
Automatic disarm test only	The disarm test starts automatically when the system is disarmed. No arm test is available.

Output controllers

Specify the number of output controllers attached to the control panel. This does not include output controllers attached to system DGP devices.

Zone event text word

Range: 0 to 999

When zones 57 and 58 are active, the zone event text word will be displayed on all system LCD keypads. The zone event text word can be either a text word from the word library or a user-defined text word.

Number of prefix digits

Range: 1 to 4

The alarm code prefix enables user codes to be used for both access control and alarm control. The prefix indicates the number of digits that have to be entered to have alarm control. If those digits are not entered (left blank), only access control may be performed.

For example, if the alarm code prefix is two digits, and a users PIN code is 123456, then 123456 will be entered for alarm control or 3456 for access control.

LCD rotation speed

Range: 0 to 15

Specify the rotation speed for text displayed on LCD keypads. The default value is 8. Any value from 9 to 15 decreases the text rotation speed. Any value from 1 to 7 increases the text rotation speed.

Time before rotate

Range: 0 to 15

Specify the time before LCD text starts to rotate. The default value is 8. Any value from 9 to 15 increases the time before text rotation starts. Any value from 1 to 7 decreases the time before text rotation starts.

User offset

Range: -65536 to 65536

The user offset provides the ability for the control panel to adjust the numeric value of user numbers being reported to the management software. The number entered will be

added (subtracted if it is negative) to the user number in the control panel and sent to the management software. This can be used in conjunction with the system code offsets.

This option is of particular benefit to the management software administrator. A typical application would be to have numbers appearing in reports conform to a specific numeric range.

End-of-line (EOL) resistor

Range: 10K; 4.7k; 2.2k

Specify the value to set the type of end-of-line resistor that is used in the system.

Duress type

Specify the duress type to use to activate the duress function. The duress function activates a silent signal to alert security personnel via the central station.

For example, if a user is forced under threat to disarm the system, they can enter a disarm code plus duress code to disarm the system and silently send a duress signal to the central station.

Increment last digit. A duress digit in conjunction with the PIN code is used. The duress digit is the last digit of the PIN, plus one (1). If the last digit of the PIN code is 9, then the duress digit is 0.

For example, if the user's PIN code is 1234, the duress digit will be 5. To disarm the system and active the duress signal the user will enter 12345.

Add zero to end. If the user adds a zero to their PIN code the duress signal is sent to the central station.

For example, if the user's PIN code is 1234, the duress digit will be 0. To disarm the system and active the duress signal the user will enter 12340.

Siren type

Specify the one of the following siren types:

Standard (speaker tone). The 16th output is activated and a saw tooth signal is generated at the siren output.

Volts on. The 16th output is activated and a constant DC voltage is set at the siren output.

Programmable tones (speaker or volts). The 12th, 13th, 14th, 15th, and 16th outputs are mapped to the siren output. These outputs have priority 1 to 5 respectively. Therefore, output 12 will have a higher priority than output 16 when both are active, thus generating a DC voltage at the siren output.

Table 33 shows the type of output generated when the programmable tones siren type option is selected (different outputs are activated.)

Table 33. Outputs generated

Output	Generates
12th	Constant DC voltage at the siren output
13th	A warble tone at the siren output
14th	A saw tooth tone at the siren output
15th	Two tones at the siren output
16th	An inverted saw tooth tone at the siren output

Alliance system code

Range: 0 to 65536

Specify an optional system code assigned to the control panel. This code is only useful if the installer would like to make it difficult to perform engineering resets by the end users. This code is input into an equation in order to generate the reset code.

Because the reset code is determined by two sets of values, this option makes it much more difficult to perform and engineering reset and consequently add more security to the system.

System codes A and B

Specify the system codes for this control panel. The control panel will only accept user cards with these codes. Type a code from 1 to 10 digits in length, or type 0 (zero) to specify no code.

There are two system codes (A and B), which allow the control panel to accept two sets of cards with different system codes.

Offset A and B

Range: -32767 to 32767

Specify the number to be added or subtracted from the actual user card ID number. The control panel will calculate the user number using the following calculation:

User Number = CARD ID + (or -) card offset

The calculated user number is used for programming the user and when reporting events to the central station, or the computer.

Offset A and B is used in conjunction with the respective system code. System code A is mapped to Offset A and System code B is mapped to Offset B.

Soak test days

Range: 1 to 255 days

Specify the number of days for the soak test period. The soak test period is started when *enable soak test* is set in *Zone programming*. If soak test days is left blank, the soak test period is infinite and must be disabled by the user.

The soak test can be used to diagnose problems without causing false alarms. When a zone is set to soak test, it **does not**:

- Report to central station
- Activate siren
- Activate strobe
- Activate any outputs (relays)

The change of the zone state is logged in the history file with events soak alarm and soak alarm restore. If the zone does not go into alarm during the soak test period, the enable soak test option for that zone will be reset when the soak test period has elapsed. If the zone goes into alarm during the soak test period, the soak test period is extended by the amount of time specified in soak test days.

System options

Dual zone	**Enabled**: Dual zone operation is activated. For dual zone to operate every zone needs two 4k7 resistors, enabling the panel to detect whether a zone is in a normal state, active or tampered. This is a global setting and affects all zones. **Disabled:** Dual zone operation is disabled.
Automatic unbypass when area disarmed	**Enabled**: Zones in a normal bypassed state are unbypassed when any of the areas assigned to the zone are disarmed. This ensures that bypassed zones are not ignored or overlooked during disarm. This option is only valid if the alarm group is programmed for the *automatic unbypass* option in *Alarm groups programming*. **Disabled:** Zones are not unbypassed when areas assigned to the zone are disarmed.
Display one zone at a time	**Enabled**: One zone at a time is displayed on the LCD keypad even though there may be more than one in the list of zones to be displayed. The user must scroll through the zones to view them all. **Disabled:** Zones are displayed as a list of numbers and it is necessary to select the zone number to display the individual zone name.
User name file	**Enabled**: Prompts for the user name when programming user codes using the LCD keypad. **Disabled:** Will not prompt for the user name when programming user codes using the LCD keypad.
System alarms set siren and strobe	**Enabled**: The dedicated tamper zones on the control panel and the DGP devices activate the siren and the strobe when in alarm. **Disabled:** The dedicated tamper zones do not activate the siren and strobe when in alarm.
Latching systems alarms	**Enabled**: System alarms latch and require a code to reset them. This ensures that users, who have the appropriate authority, are assigned an alarm group that has *reset system alarms* enabled in *Alarm groups programming*. **Disabled:** System alarms automatically reset and report the restore when the alarm condition is no longer present. System alarms include RAS (arming station) or DGP offline, cabinet tamper, siren tamper, AC fail, fuse fail, and low battery.

Siren testing	**Enabled**: Enables a siren test for three seconds when the arm test is started. **Disabled:** Sirens are not tested when the arm test is started. Refer to *Siren type* option.
Disable "0 ENTER" for camera reset	**Enabled**: Users cannot enter **0 ENTER** on an LCD keypad to stop cameras operating. The cameras continue to operate until someone who is authorized to control cameras resets them. **Disabled:** When a user enters **0 ENTER** on an LCD keypad, the camera operating is stopped.
Disable insert of alarm group restriction	**Enabled:** Disables the option to treat areas as vaults. By disabling this option, the non-vault areas will not be automatically armed. **Disabled:** Ability to treat areas as vaults is enabled. See *Alarm group restrictions* on page 197.
Disable code for displaying	**Enabled**: The PIN code is not displayed when programming a user on the LCD keypad, instead the display shows *PIN codes can not be viewed*. **Disabled:** User PIN codes are displayed when programming users on the LCD keypad.
Disable flashing area LEDs	**Enabled**: The area LED on system keypads will not flash when there is an alarm and/or tamper alarm in a given area. **Disabled:** Keypad area LEDs will flash when there is an alarm and/or tamper alarm in a given area.
Two users for user programming	**Enabled**: Two users are required to enter their PIN codes before access is granted to program users. This does not apply to the Master user account. **Disabled:** Only standard PIN code access is required to program users.
Display alarms instantly	**Enabled**: Alarm details are displayed immediately on LCD arming stations after an alarm has taken place. **Disabled:** Alarm details are not displayed immediately on LCD arming stations after an alarm has taken place. To view alarms on the LCD arming station, you must press **ENTER** on the key pad twice.
Siren only after fail to report	**Enabled**: Siren event flags are only activated on alarms if the control panel has failed to report to the central station. Fail to communicate (FTC) is registered at the end of the fourth dial attempt. The siren activates for the normal siren cutoff time programmed. **Disabled:** Sirens will operate on related alarms.

Financial options	**Enabled**: Activates three special options (generally applicable to financial institution installations). 1. Film counters are enabled during the disarm test mode. 2. Alarm group restriction 2 or alarm group restriction 6 disables delayed disarmed alarm zones. See *Alarm group restrictions* on page 197. 3. Minimum PIN code length is set to 5 digits. **Disabled:** System operation is normal.
Enable buzzer on AC/line fault	**Enabled**: The keypad buzzer will be sounded when there is an AC/line fault. **Disabled:** The keypad LED will flash upon an AC/line fault.
Enable call central station display	**Enabled**: System LCD keypads indicate that the system has successfully reported and/or is currently contacting the central station with the report of a burglar alarm or tamper activation. **Disabled:** System LCD keypads will not indicate successful burglar alarm or tamper activation reports to the central station.
Enable log limitations	**Enabled**: Limits the number of times a zone can log and report a change-of-state event within the same arm/disarm cycle. The zone log limit is set to three change-of-state event reports. **Disabled:** No limit is imposed on zone logging.
Indicate bypassed zones	**Enabled**: Alerts the user at the RAS device with an optical and audible indication that zones are bypassed in an area that is being armed. The bypassed zones will be listed and the user prompted with the option to arm the system. **Disabled:** The RAS device will not indicate bypassed zones.
Display user flags	**Enabled**: Special user flags are displayed when programming users. The special user flags include two card function, guard, visitor, trace user, card only, privileged, and extended access. **Disabled:** The special user flags are not displayed.
Delayed disarmed alarm lockout	**Enabled**: An alarm can only be cancelled if the zone is in a normal state. Delayed disarmed alarms are locked out until the alarm device is reset (and the zone has switched to a normal state). This only applies to latching delayed disarmed alarms. **Disabled:** Normal operation. Delayed disarmed alarms are not locked out.

Zone expansion fitted	**Enabled**: Indicates that an 8-zone expander is attached to the control panel. **Disabled:** Indicates that an 8-zone expander is not attached to the control panel.
Bypass zone tamper	**Enabled**: When a zone is bypassed, the tamper is also bypassed. No tamper alarm will occur. **Disabled:** Tamper alarms will occur normally.
Report multiple alarms	**Enabled**: Reports multiple alarms as a separate alarm for each alarm that occurs. **Disabled:** Only the first alarm will be reported. Any following alarms that occur will not be reported.
Report multiple restores	**Enabled**: Reports a restore for every alarm that occurs. **Disabled:** Reports only one restore for every zone that generates an alarm.
Engineer reset on system alarms	**Enabled**: After a system alarm, an engineer reset is required. A user cannot arm any areas until an engineer reset is done. **Disabled:** Areas can be armed after a system alarm without an engineer reset.
Engineer reset on system tampers	**Enabled**: After a system tamper alarm, an engineer reset is required. A user cannot arm any areas until an engineer reset is done. **Disabled:** Areas can be armed after a system tamper alarm without an engineer reset.
Arm with no battery	**Enabled**: The control panel will arm without a battery attached. **Disabled:** the control panel will not arm if the battery is missing.
User can do engineer reset	**Enabled**: A user can do an engineer reset. The user has to give the code that is shown on the display to the installer who can then find a reset code. **Disabled:** An engineer reset can only be done by using a dedicated zone 65 or through the LCD keypad installer programming menu.

Engineer entry protect	**Enabled**: A user can only enter LCD keypad installer programming by opening the box tamper within 120 seconds. This displays 'Open box tamper' on the LCD keypad. During the 120 seconds or when in the installer menu, the box tamper alarm will be disabled. When the installer menu is exited, the installer has 120 seconds to close the box tamper before the tamper alarm is activated. This is used to protect against unauthorized entry by an installer. **Disabled:** An authorized user can always enter LCD keypad installer programming. Opening the box will always cause a tamper alarm.
Send arming after exit	**Enabled**: When armed, an area will defer the reporting of arming to the central station until the exit time has ended. **Disabled:** An area will not defer the reporting of arming to the central station.
Bypass alarm reporting on exit fault	**Enabled**: Bypasses reporting of alarms with a reporting code of 17-24 (burglar alarm) when the exit timer is running. Alarms that occur during the exit time will set the exit fault flag and disable further alarms on the assigned areas until the areas are disarmed. **Disabled:** Alarms are reported immediately.
Disable tamper reporting in disarm	**Enabled**: Zone tamper and restore events will not report to the central station if the assigned areas are disarmed. If a tamper occurs while disarmed, the action will log. **Disabled:** Zone tamper and restore events will report to the central station if the assigned areas are disarmed.
Bypass external siren and strobe for tamper in disarm	**Enabled**: Zone and system tampers will only activate the internal siren. **Disabled:** Internal and external sirens and the strobe will activate as a result of tamper events.
Installer dual code	**Enabled**: Two users are required to enter their PIN codes to enable installer programming. The second code must be a valid user code with no access to the installer menu. **Disabled:** Two user PIN codes are not required to enable installer programming.

Custom LCD message

The custom LCD message allows you to modify the text displayed on the RAS devices connected to the control panel. You may enter up to 32 characters for this text. You will only see this text displayed on the RAS device if there are no alarms or system messages.

Programming

The following programming option is available for the custom LCD message feature:

Text

Specify the 32 characters of customized text that will be displayed on the LCD arming station (RAS) in place of the normal Alarms display. The 32 characters can include numbers, spaces, or punctuation but the following characters are **not** allowed:

~ @ ^ ` {

Event Flags

Event flags are used by the system in order to signal an event. When a certain event occurs event flags are raised to notify other programming options to perform a specified function. Below are a few common event flag uses.

Relays. Relay programming associates an event flag with a physical/logical relay. When the event flag is raised, the relay will fire.

Doors. Each RAS device supports a door event flag that is raised whenever a user is granted access.

Macro logic. Macro logic uses event flags in AND/OR logic sequences. For example, a macro might require two event flags to be true/active to raise another event flag and cause a specified action.

Internal/external sirens. Zone programming supports the ability to raise an event flag that causes the control panel to sound a siren.

System events. Raise an event flag whenever an A/C failure takes place.

In general, event flags fall into two categories, predefined and custom event flags.

Predefined event flags

The system predefines 16 event flags that are primarily used in area programming. Table describes these predefined event flags.

Table 34. Predefined event flags

Event flag number	Event flag name	Description
1	External siren	Flag is raised when any external siren activates in any area.
2	Armed alarm	Flag is raised when a zone generates an alarm and all areas assigned to the zone are armed. It is also used to activate the system strobe by default.
3	Armed alarm	Same as event flag 2.
4	Armed alarm	Same as event flag 2.
5	Armed alarm	Same as event flag 2.
6	Disarmed alarm	Flag is raised when a zone generates an alarm and one or more of the areas assigned to the zone are disarmed.
7	Disarmed alarm	Same as event flag 6.
8	24 hour alarm	Flag is raised when any zone generates an alarm.
9	Armed alarm	Same as event flag 2.
10	Armed alarm	Same as event flag 2.
11	Armed alarm	Same as event flag 2.
12	Armed alarm	Same as event flag 2.
13	Internal siren	Flag is raised when any internal siren activates in any area.
14	N/A	Do not use.
15	N/A	Do not use.
16	Testing	Flag is raised during the arm test. The flag will remain active for 50 per cent of the *testing event flag time* option in timers programming.

Enabling certain options in zone programming will cause these flags to be raised.

Example. Enabling the *external siren* option in *Zone programming* will cause the external siren event flag to be raised during an alarm condition.

Event flag description. Defines event flag number 1 as external siren.

Area. Allows the user to associate an event flag number with the *external siren event flag* option in *Area programming*. In this case, event flag number 1 is assigned.

Zone. Supports an option that will sound the external siren if the zone goes into alarm. When the zone does go into alarm, the system will first determine if the siren event flag should be raised. If the option is enabled, the system will fetch the event flag from the assigned area, and raise it. Once that particular event flag is raised, the system will then sound the alarm because there is an understanding within the system that the external siren will be activated whenever event flag number 1 is raised.

Custom event flags

Custom event flags are typically used in options such as macro logic programming and RAS programming. For example, the *door event flag* option in *RAS programming* is raised whenever the RAS device grants access to a user.

Event flag description

Event flag descriptions are used to fully describe the meaning of the custom event flags. They should be used so that any installer can easily understand the purpose behind each event flag, especially when it comes to programmable logic (Macros).

Functions

Event flags can be used for the following functions:

Readability . Event flag descriptions make it easier for installers to read/understand the event flag.

General programming. While setting up the system, numerous programming options offer the ability to choose an event flag. The process of assigning an event flag for these options is significantly easier when you have a clear description of the event flag rather than just an event flag number.

Programming

The following programming options are available for event flags:

Event flag number

Range: 1 to 255

Specifies which event flag is being programmed.

Description

A 40-character text description. The description is not transferred to the device, and is only used by the management software.

System event flags

System event flags deal with system-level events. When the specified conditions occur, the system will cause the programmed event flag to be raised. The system event flags will latch if the *latching system alarms* option is enabled in *System options programming*. Do not assign any of the 16 predefined event flags to any of the system event flags and ensure that the event flags assigned are not used in other programming options (areas, zones, etc.).

Functions

System event flags can be used for the following functions:

System level monitoring. Associate custom event flags with system events.

Indicators. Provide a visual indication when specified events take place. For example, use an LED to indicate that the computer connection is OK.

RAS keypad buzzer. Cause RAS devices to sound their warning buzzer.

Programming

Table 35 shows the programming options available for system event flags.

Table 35. System event flag programming options

Event flag	Description
AC fail	Flag is raised when an AC failure condition exists on the control panel or any DGP.
Low battery	Flag is raised when a low battery condition exists on the control panel or any DGP.
Fuse fail	Flag is raised when a fuse fail condition exists on the control panel or any DGP.
Tamper	Flag is raised when a tamper condition exists on the control panel or any DGP.
Siren fail	Flag is raised when a siren failure condition exists on the control panel or any DGP.
DGP bypassed	Flag is raised when a DGP has been isolated via the bypass/unbypass command. See *Alarm groups* on page 188.
DGP offline	Flag is raised when a DGP has been programmed to be polled by the control panel, but is not responding.
RAS offline	Flag is raised when a RAS device has been programmed to be polled by the control panel, but is not responding.
Duress	Flag is raised when a keyboard duress alarm occurs.
Filmout	Flag is raised when the film count for a camera exceeds the programmed Film Out level. The *film out* option is programmed in *System options programming*.
Report fail – fail to communicate (FTC)	Flag is raised when the control panel fails to report to the central station. FTC is initiated after the fourth attempt.
Test mode	Flag is raised when the control panel is in test mode.
All armed	Flag is raised when no areas are disarmed, there are no alarm conditions, and no entry/exit timers running.

Table 35. System event flag programming options (continued)

Event flag	Description
Keypad buzzer	When the assigned flag is raised, the keypad warning beepers are activated.
Dialer is off-hook/active	Flag is raised whenever the dialer is off-hook. Since not all reporting is via PSTN, *dialer active* more accurately represents this event.
External siren test	Flag is raised during the external siren test. This event flag could then be used to switch a relay to disconnect the siren auxiliary power for testing.
All armed pulse	Flag is raised when the system is fully armed. Each of the following criteria must be true in order for the system to raise the flag: • All areas with inputs assigned are armed • No alarm conditions (no inputs isolated) • No entry/exit timers are running
Computer connection active	Flag is raised when the connection between the control panel and the management software is active.
Line fault	Flag is raised during line fault conditions. The control panel will constantly monitor the line determined by *Central station communications programming* to determine if the line is in fault.
Battery test	Flag is raised during battery test.
Engineer walk test running	Flag is raised during an engineer walk test.
Engineer walk test reset	After each walk test, a new engineer walk test reset system event flag will be activated for 5 seconds.

Text words

Text words provide the functionality to display descriptive names for system resources, such as zones and alarm groups, on the LCD keypad. By default, the system provides up to 900 predefined default text words in the text word library (see *Text word library* on page 308). You can also add up to 100 user-defined text words to customize the library to your specific needs.

Not all system resources use text words. For instance, although DGP programming supports a description property, this is not treated as a text word, nor is it downloaded to the panel. Therefore the DGP description will not be shown on the LCD keypads.

When creating a name for a system resource that does use text words, the existing text word library is searched for any matches in the resource name and existing text words are used. If, however, the words contained in the name/description do not exactly match one of the predefined words, you can add a user-defined text word. The *Text word* tool on the toolbar provides a searchable list of both predefined and user-defined text words.

Functions

Text words can be used for the following functions:

Resource naming. Text words allow system resources to have associated custom names, which are reported on LCD keypads for ease of use and clarity.

Reporting. System resources with text word names will show the text word name for reporting and logging.

For example, if zone 1 was assigned the text word *Front Door Main Entrance Zone* and the zone is in alarm, then that exact zone name is reported, along with the zone number.

Under most circumstances, text words are limited to 16 characters. Zones, however, allow up to four text words and four numbers. The above example incorporates more than one text word.

Programming

The following programming options are available for text words:

Text word number

Range: 900 to 999

Specify the user-defined text word number.

Control panel number

Specify the control panel that is associated with this user-defined text word.

Description

Range: 1 to 16 characters

Specify the text word description to be stored in the user-defined word library. The description can include spaces, for example, Joe Doe Security.The following characters are not allowed: ~ @ ^ | \ {

Chapter 16 Maintenance and support

This chapter provides information on maintenance procedures and technical support contact information.

In this chapter:

Maintenance

Alliance Builder relies on specific data sources and files to store data. It is essential that these data sources and files remain intact at all times. Alliance Builder automatically manages these data sources, their locations and relationships with no action required by the user. However, if data sources are changed, or data files removed, the relationships that Alliance Builder relies on will be broken and may result in lost projects.

A brief explanation of the data sources, files, and relationships that Alliance Builder uses to store data is provided in the following sections.

MSDE database

Alliance Builder uses Microsoft's MSDE database engine to store application data as well as projects created in Alliance Builder. Alliance Builder relies on the database to store information about project file locations, properties for devices that have been created and much more. All information stored in the MSDE database is managed by Alliance Builder and is not intended to be modified by the user in any way. Any modifications to the database and the data it contains could adversely effect projects that have been created in Alliance Builder or may even effect the overall operation of Alliance Builder itself.

CPD files

Alliance Builder uses CPD files to store project programming information. A CPD file is created for each control panel that is added to a project, so there is a direct relation between the number of control panels in a system and the number of these files that exist for a project. The files are stored in the project directory chosen when a new project is created and are managed by Alliance Builder. CPD files should never be moved, removed, or edited by the user in any way. All interaction with these files should occur automatically from within Alliance Builder.

APF archive files

Alliance Builder 8200 APF archive files are used when exporting or importing projects. Alliance Builder uses information stored in the MSDE database as well as information stored in the CPD files to create an APF archive. The archives contain all necessary programming and project information for a project to be transferred to Alliance 8100,

Alliance 8300, or another Alliance Builder 8200. If any information for a project is moved or removed from the database, or if required CPD files are moved or removed, the APF archive file will not be complete and will not contain all of the necessary project information.

Recommended practice

Alliance Builder requires information stored in the MSDE database and the project CPD files to function correctly. Alliance Builder manages this information and the location of these files, so no user interaction is required. Users should not modify or manipulate data stored in the MSDE database or project CPD files in any way. A safe approach is to restrict users to only interact with Alliance APF archives. Alliance APF archive files are intended to be moved or removed by the user and will not effect Alliance Builder operation and project integrity if they are manipulated.

Contacting technical support

For assistance installing, operating, maintaining, and troubleshooting this product, refer to this document and any other documentation provided. If you still have questions, you may contact technical support during normal business hours (Monday through Friday, excluding holidays, between 6 a.m. and 5 p.m. Pacific Time).

Table 36. Sales and support contact information

	Sales	Technical support
Phone	**Toll-free:** 888.GESECURity (888.437.3287 in the US, including Alaska and Hawaii; Puerto Rico; Canada). Outside the toll-free area: 503.885.5700.	
E-mail	`info@gesecurity.com`	`generaltech@ge.com`
Fax	800.483.2495	**541.752.9096** (available 24 hours a day)

Note: Be ready at the equipment before calling for technical support.

Online publication library

Another great resource for assistance with your GE product is our online publication library, available to all of our customers. To access the library, go to our website at the following location:

`http://www.gesecurity.com`

In the **Tools** area at the top, click the *Publication Library* link. After you register and log on, you may search through our online library for the documentation you need.[1]

1. Many GE documents are provided as PDFs (portable document format). To read these documents, you will need Adobe Acrobat Reader, which can be downloaded free from Adobe's website at `www.adobe.com`.

Appendix A Boolean logic

This appendix provides an overview of Boolean logic and examples of macros applied to Boolean logic.

Boolean logic

A Boolean logic equation consists of three basic components, inputs or operands, operators, and a result X. The Alliance system applies Boolean logic to create macros.

Inputs (operand). An input, in a logic equation, can have only one of two possible values or states. Some examples of the logical state of an operand is True or False, Set or Clear, Off or On, 1 (one) or 0 (zero), Active or Inactive, and Yes or No. In the Alliance system for instance, a zone alarm event flag is set or clear, it is true if in alarm and false if not in alarm.

Result X (output). The result of the equation is based on the operations performed on the inputs (operands). The value of the result is either true or false. If true, the macro will be performed.

Operators. Operators perform logical operations on the inputs (operands). These operands can be considered logic gates with multiple inputs and a single output. Each operator can be called a gate, such as *OR* gate or *AND* gate. When defining a macro within the Alliance system, it is beneficial to understand the symbols of a gate and how it is wired into the logic.

Logical *OR* operator

The *OR* operator performs a logical OR on the inputs and can be summarized as any 1 in results in a 1 out, or any true input will result in a true result.

If A or B are active, then the result X is active. In *Table 37* for the OR gate symbol, the notation for an OR operation is +, as in *A + B* and is said *A OR B.*

A OR B = X

Table 37. OR gate

Input A	Input B	Output X
False	False	False
True	False	True
False	True	True
True	True	True

Logical *AND* operator

The AND operator performs a logical AND operation on the input and can be summarized as an 0 results in a 0 out.

In *Table 38* for the AND gate symbol, the notation for an AND operation is *, as in *A * B* and is said *A AND B*.

A AND B = X

Table 38. AND gate

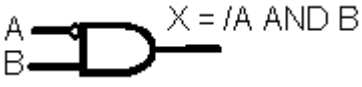
Input A	Input B	Output X
False	False	False
True	False	False
False	True	False
True	True	True

Logical *NOT* operator

A NOT can be applied individually to an input or any output of a gate. Essentially the operation inverts the state, a NOT true equals false, either going into the gate or out of the gate.

Inverter NOT symbol

In the inverter NOT symbol, notice that the / notation preceding the *A* in *X = /A* indicates that the value of X (output) is the opposite of A (the input). The bubble is actually the inverter and as such can be applied to any input to any gate or output of any gate, as in the following figure:



The notation for a NOT operation is / as in */A * B* and is said *NOT A AND B*. To have a true output X, A must be false AND B must be true.

/A * B = X

Table 39. NOT gate

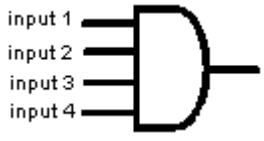
Input A	Input B	Output X
False	False	False
True	False	False
False	True	True
True	True	False

Combination logic

The Alliance system allows the user to define macros with up to four logical inputs, each having three basic operators with one output. In some situations it may be that all inputs are OR gated or AND gated resulting in the following figures.

Input OR gate

Input AND gate



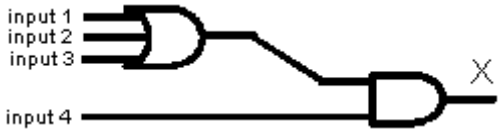
These are logic equations of the simplest form. To have a positive output on the 4 input OR gate any one of the four inputs needs only be true or positive. However, all inputs to the AND gate must be true to have a true output.

Many macros consist of a combination of gates to drive an output and the programmer must have a basic understanding of how to use a combination of logic gates to drive the output. Each input will have the ability to be OR gated or AND gates with the following input.

(1 AND 2) OR 3 OR 4 = X

This logic function with inputs 1 and 2 AND gated results in the gate providing one input to a 3 input OR gate. If either 3 or 4 are true the output will be true. If both inputs 1 and 2 are true, the output will be true because the output of the AND gate for inputs 1 and 2 are OR gated to the result.

(1 OR 2 OR 3) AND 4 = X



Input 4 must be true and any one of inputs 1, 2, or 3 must be true for X to be true. Input 4 enables any of the OR gated inputs to drive X.

Examples of macros applied to Boolean logic

The following examples are guidelines to help you create macros and map them to the underlying Boolean logic.

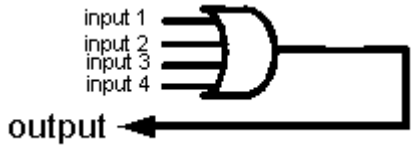
Example 1. 4 input OR gate

Table 40. Example 1

Input	OR/AND	Result
1	OR	If any of the inputs activate, collectively, or individually, the output will be triggered.
2	OR	
3	OR	
4	OR	

The inputs are activated by an output (relay) activating or an event flag activating. All inputs may be optionally individually inverted, the NOT function. Any unused inputs should be set to OR. The logical equation can be combined with any output function except for the latched output function.

Logical symbol



Logical equation. Input 1 + Input 2 + Input 3 + Input 4 = Output

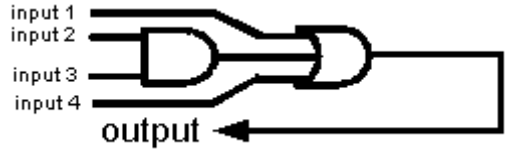
Example 2. 2 input AND gate + 2 input OR gate combined

Table 41. Example 2

Input	OR/AND	Result
1	OR	If input 1activates, the output will be triggered.
2 3	AND AND	If inputs 2 and 3 activate, the output sill be triggered.
4	OR	If input 4 activates, the output will be triggered.

The inputs are activated by an output (relay) activating or an event flag activating. All inputs may be optionally individually inverted, the NOT function. Any unused inputs should be set to OR. The logical equation can be combined with any output function except for the latched output function.

Logical symbol



Logical equation. Input 1 + (Input 2 * Input 3) + Input 4 = Output

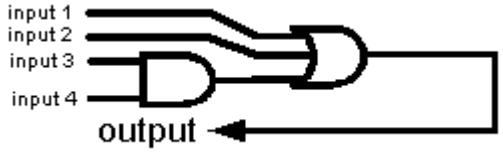
Example 3. 2 input AND gate + 2 input OR gate combined

Table 42. Example 3

Input	OR/AND	Result
1	OR	If either input 1 or input 2 activates, the output will be triggered OR
2	OR	
3 4	AND AND	Inputs 3 and 4 have to activate simultaneously to tripper the output.

The inputs are activated by an output (relay) activating or an event flag activating. All inputs may be optionally individually inverted, the NOT function. Any unused inputs should be set to OR. The logical equation can be combined with any output function except for the latched output function.

Logical symbol



Logical equation. Input 1 + input 2 + (Input 3 * Input 4) = Output

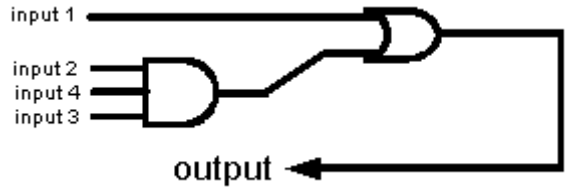
Example 4. Combination not applicable, do not use

Table 43. Example 4

Input	OR/AND	Result
1	OR	If input 1 activates, the output will be triggered.
2	AND	Input 2 NOT OPERATIONAL
3	AND	Input 3 NOT OPERATIONAL
4	AND	Input 4 NOT OPERATIONAL

Do not use this combination! The exact logical equation with different inputs can be achieved by the combination in example 6.

Logical symbol



Logical equation. Input 1 = Output

Input 2 * Input 3 * Input 4 = Not operational

Note: Alliance Builder cannot perform this combination.

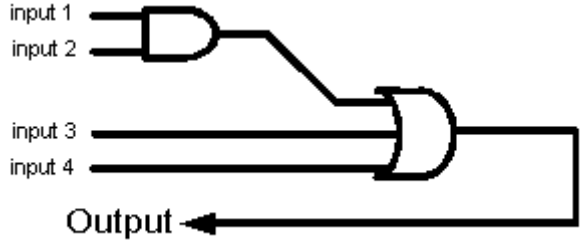
Example 5. 2 input AND gate + 2 input OR gate combined

Table 44. Example 5

Input	OR/AND	Result
1	AND	Inputs 1 and 2 must activate simultaneously to trigger the output OR
2	AND	
3 4	OR OR	Input 3 OR Input 4 will trigger the output.

The inputs are activated by an output (relay) activating or an event flag activating. All inputs may be optionally individually inverted, the NOT function. Any unused inputs should be set to OR.The logical equation can be combined with any output function except for the latched output function.These rules apply to all examples, except for example 8, the actual latched output function example.

Logical symbol



Logical equation. (Input 1 * Input 2) + Input 3 + Input 4 = Output

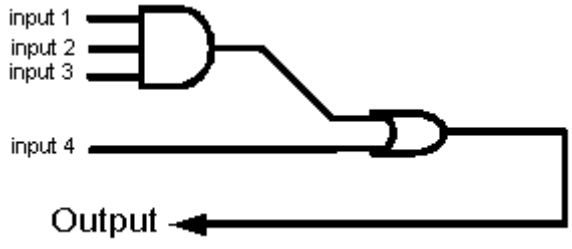
Example 6. 3 input AND gate + 1 OR input combined

Table 45. Example 6

Input	OR/AND	Result
1	AND	Input 1 AND Input 2 AND
2	AND	
3 4	AND OR	Input 3 have to activate simultaneously to trigger the output OR input 4 can trigger the output directly.

The inputs are activated by an output (relay) activating or an event flag activating. All inputs may be optionally individually inverted, the NOT function. Any unused inputs should be set to OR. The logical equation can be combined with any output function except for the latched output function.These rules apply to all examples, except for example 8, the actual latched output function example.

Logical symbol



Logical equation. (Input 1 * Input 2 * Input 3) + Input 4 = Output

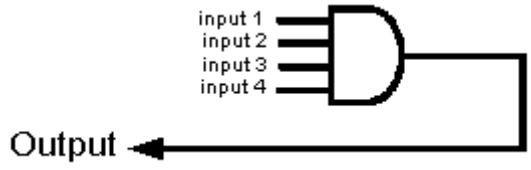
Example 7. 4 input AND gate

Table 46. Example 7

Input	OR/AND	Result
1	AND	Input 1 AND
2	AND	Input 2 AND
3	AND	Input 3 AND
4	AND	Input 4 have to activate simultaneously to trigger the output.

The inputs are activated by an output (relay) activating or an event flag activating.All inputs may be optionally individually inverted, the NOT function. Any unused inputs should be set to OR. The logical equation can be combined with any output function except for the latched output function. These rules apply to all examples, except for example 8, the actual latched output function example.

Logical symbol



Logical equation. Input 1 * Input 2 * Input 3 * Input 4 = Output

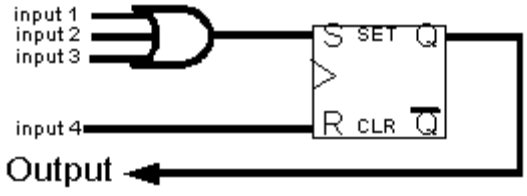
Example 8. RS flip-flop: 3 x SET inputs, 1 x RESET input

Table 47. Example 8

Input	OR/AND	Result
1 2 3	OR/AND OR/AND OR/AND	SET the RS flip-flop output SET the RS flip-flop output SET the RS flip-flop output
4	OR/AND	RESET the RS flip-flop

When the output function is set to latched, the macro is not looking at all to logical expression OR or AND for all input.The first 3 inputs will be handled as SET inputs and the fourth input will be handled as a RESET input of a RS flip-flop.The RESET will always predominate the SET inputs.Inverting the input conditions or output conditions is still applicable.

Logical symbol



Logical equation. Input 1 + Input 2 + Input 3 = SET output

Input 4 = RESET output

Commonly used macros

The following are examples of commonly used, helpful macros.

Door control using different door unlock time

Description. Door control using different door unlock time. The door unlock time (doors 1 to 16) is a global setting.

Setup

RAS event flag set	RAS EF
Event to output	Door unlock output triggers on DOOR UNLOCK EF

Macro programming

Macro output		Timed (1 to 255 seconds)
	Input flag	Timed - required time
Input 1	EF	RAS EF
Input 2	Undefined	OR
Input 3	Undefined	OR
Input 4	Undefined	OR
		Door unlock
Activate	EF	EF

Operate door when area is not armed

Description. Only allow a door to be opened when area is not armed.

Setup

RAS event flag set	RAS EF Area
Area disarmed EF	EF
Event to output	Door unlock output triggers on DOOR UNLOCK EF

Macro programming

Macro output		Timed (1 to 255 seconds)
		Timed - required time
Input 1	EF	RAS EF Area
Input 2	EF	EF AND
Input 3		
Input 4		
		Door unlock
Activate	EF	EF
Door unlock EF = RAS EF x Area EF		

Use function keys to set an output

Description. Use the function keys to set an output/arm a system using a function key.

Setup

Event to output	OPUT setup for activating on time zone 42 or above
Alarm group	Setup alarm group AGRP for area with alarm system control and arm only
Input	Input IPUT setup as type 5 using alarm group AGRP

Macro programming

Macro output		Timed (1 to 255 seconds)
		Timed - 2 seconds
Input 1	O/P	OPUT
Input 2		
Input 3		
Input 4		
Activate	I/P	IPUT

Provide latch functionality for entry/exit loop

Description. Setup an EF providing latch functionality (suitable for detectors in entry/exit loop).

Setup

Event to output	Latch OPUT triggered by LATCH EF
Area	Area disarmed EF (AREA EF) Entry EF (EE EF) Exit EF (EE EF)

Macro programming

Macro output		Non-Timed
		Area
Input 1	EF	EF Not
Input 2	EF	EF Not AND
Input 3		OR
Input 4		OR
Activate	EF	LATCH EF

Activate a buzzer when a zone is active and area is not armed

Description. Activate a buzzer when a zone is active and the area is disarmed.

Setup

System EF	Keypad buzzer triggered by CHIME EF
Area	Area disarmed EF (AREA EF)
Inputs	Zone EF IPUT EF Zone EF when active = YES

Macro programming

Macro output		On timed (1 to 255 seconds)
		Time = TIMED
		AREA
Input 1	EF	EF
		IPUT
Input 2	EF	EF AND
Input 3		
Input 4		
Activate	EF	CHIME EF

Activate buzzer when zone is active

Description. Activate a buzzer when a zone is active and the area is disarmed but only out-of-hours.

Setup

System EF	Keypad buzzer triggered by CHIME EF
Area	Area disarmed EF (AREA EF)
Inputs	Zone EF IPUT EF Zone EF when active = YES OOH time zone Out-of-hours
Time zones	time zone OOH
Event to output	OP Triggers on IPUT EF Disabled by OOH time zone

Macro programming

Macro output		On-timed (1 to 255 seconds)
		Timed - TIMED
		AREA
Input 1	EF	EF
Input 2	O/P	OOH OP EF AND
Input 3		
Input 4		
Activate	EF	CHIME EF

Appendix B Card access

This appendix provides an overview of how the Alliance system uses card readers for access control. Alliance provides user input through personalized cards for each user that has access to the areas controlled by the system.

In this appendix:

Card and card reader types

There are three basic types of cards and card readers.

Magnetic swipe. Magnetic scope cards have a magnetic strip along the edge of the card that contains encoded information about the user. The information is communicated when the card is moved through the card slot of the reader. The information stored on these cards must be specified during the purchasing process. The Alliance system currently supports several magnetic readers and keypads.

Wiegand. Wiegand proximity cards have user information embedded on the card. This information must be specified during the purchasing process. The cards are read by placing them in close proximity to a Wiegand reader.

Smart cards. Smart cards allow the Alliance administrator to program access cards through an Alliance management software program. These cards can be reprogrammed as needed. Smart cards are read by placing them in close proximity to a proximity card reader.

Card formats and data fields

When a card is read by a reader, the system code and the card number are communicated. Depending on the type of card used, this information is either embedded on the card when purchased, or programmed by the Alliance smart card programmer.

The following types of formats can be used with an Alliance system:

magnetic swipe card. System code range from 0 to 65535, card number range from 0 to 65535.

26-bit Wiegand. System code range from 0 to 255, card number range from 0 to 65535.

27-bit Tecom Wiegand. System code range from 0 to 247, card number range from 0 to 65535.

Smart card. Aritech Wiegand ASC (recommended), 26-bit Wiegand

Smart card programming

When a smart card is purchased, it has no embedded information and must be programmed to communicate with the reader. To program smart cards, you use an Alliance management software program and a card programmer. The programming password and the site codes are two key elements that you must know prior to programming. You must also have a basic understanding of the Alliance system.

Smart card programming options include:

Com port. Specify a Com port that has been designated as a card programmer port. If no port has been designated, identify a Com port.

Connection password. A connection password is required to connect the card programmer so that unauthorized cards cannot be programmed. This password can be any numeric password up to 10 characters in length.

Poll rate. The poll rate allows you to specify how often Alliance will poll the card programmer. We recommend a setting of 100.

Activate programmer. When you activate programmer, you allow the programmer to operate.

Master overwrite password. This password can be any numeric password up to 10 characters in length and is blank by default. This password is required in the following situations:

- When a new card for a user is created and that user already has a card issued.
- When a request is made to rewrite data to a card that already has data.

This password can only be changed by operators with the correct security access.

The connection and master passwords are stored in the card programmer and, although initially blank, will after programming require the existing password to program a new password.

Reader configuration cards

Reader configuration cards allow an operator to specify the access settings needed for the readers and write all the necessary data to one particular card. The operator can then move around the building, badging at readers that need to be programmed. This will default each reader to the information settings stored on the configuration card. The information on the card can also be read back and rewritten to allow your settings to be changed when necessary. Factory-set default settings are also available.

Reader settings include:

Valid card beep. Sound one beep when a valid card is badged in addition to other beeps that will sound due to control panel operation, such as four beeps for a valid card.

Watchdog. Transmit a watchdog data stream when in offline mode when no valid card is present.

Read option card. The smart card reader can be set up using a configuration (option) card. To disable changing the configuration more than once with a configuration card. Disable this option.

Online blue LED options. The setting of the blue LED operation when online can be changed between *Door open only* and *Disarmed plus door open*.

Online red LED options. The setting of the red LED operation when online can be changed between *Armed* and *Armed plus door open*.

Offline LED options. When offline, the LEDs can be controlled using a one-wire or two-wire operation.

Valid card LED flash. Allows the blue LED to give a short flash when a valid card is badged (on during credit transactions).

Night light. Allows the blue LED to partially light up to show directions in a dark room. When the red or blue LED is active, the night light will be off.

Reader address. Set the RAS address for this reader. When not set, only the other options will be programmed. The RAS must be polled before the reader can be used.

Protocol options. The smart card reader supports the following formats to transmit data:

- Aritech Wiegand ASC

- Magnetic swipe (clock data)

Door output. The smart card reader has an open collector output available (the violet wire) that can be activated by one of the following events:

- Door output door event flag is active on a valid card being badged.
- Tamper output RAS tamper is active.
- Card present output (magnetic swipe only) card is badged.
- Credit output timed on a valid credit transaction activates the output for a set period as programed in the output time factor.
- Credit output latched on a valid credit transaction toggles the output. The next transaction will reset it.

Request-to-exit control. Set the supports for request-to-exit. Request-to-exit is available only in online mode and uses the LED 2 input. When connected to ground, the door will open. The output option has to be set to door output.

Security mode. The security mode is used to determine if programmed smart cards with credits and user-defined cards can be read, or only blank, unprogrammed cards with a unique serial number and user-defined cards. To use the unsecured mode, a special memory module is required.

Reader token values. A token is a value representing dollars, cents, time, or just a number. You can set how many credits equal one token. For example, at a library photocopier, each time a letter-sized copy is made with the card, one token worth ten cents is deducted. While for legal size copies, two tokens are deducted.

Reader credit account number. Credit account number to subtract the used token values from (one of four available). See also credit units.

Reader location number. Select a reader location number from 1 to 4. The location number may represent an area, floor, group of floors, building, or group of buildings.

Output time factor. The output time factor is used to modify the pulse width output of the credit output pulsed option. The output time factor is in a range from 1 to 256. The pulse for the *Credit output pulsed* is the output time factor multiplied by 0.01 seconds. This gives a pulse width in the range from 0.01 to 2.56 seconds. The activation time for the *Credit output timed* option is the output time factor multiplied by the token value of the reader. This gives a time in the range of 1 second to 193 days.

System codes

A system code, sometimes referred to as a facility or site code, is a numeric value stored in the control panel and on access cards. The Alliance system has two system codes, A and B. This allows the use of cards with different system codes.

Offset

The offset is a numeric field that is stored in the system and is used to link to the card owner. Each card communicates a unique card number. Offsets range from -32767 to 32767 and specify the number to be added or subtracted from the actual user card ID number. The control panel will determine the user number using the following calculation:

User number = Card ID + (or-) card offset

Example. The card offset is programmed as -5000. The actual physical card ID number is 5001. The card will be programmed as User 1 and will report as User 1.

The calculated user number is used for programming the user and reporting events to the central station or control panel. A and B are used in conjunction with the respective system code. System code A is mapped to offset A and system code B is mapped to offset B.

IUM (intelligent user module) and memory

The hardware memory configuration of the Alliance system will determine the capacity of resources available. The largest impact is in consideration to the amount and types of users. When designing your system this factor must be taken under consideration.

The following types of hardware memory configurations can be used in an Alliance system:

- Standard (no memory expansion)
- 1 MB expansion software IUM
- Expanded 1 MB (non-IUM)
- 4 MB IUM (SIUM)
- 8 MB IUM (LIAUM)

Systems can be upgraded by ordering the memory upgrade kits. The type of configuration must be consistent throughout the Alliance system. This includes all controllers that come with a memory module such as control panels and 4-door/elevator controllers. Where systems include both, both must have the same memory configuration.

Each type of memory configuration has limitations on users and user types. There are also software IUM options only available with firmware versions F and above.

Table 48 shows the limitations for each type of memory configuration.

Table 48. Memory configuration limitations

	Standard	1 MB expansion software IUM	1 MB expansion module	4 MB IUM module	8 MB IUM module
Users with cards	50	2000	2000	17873	65535
Users with names	50	200	200	200	200
Users with PINs	50	2000	1000	1000	1000
Alarm events	250	1000	1000	1000	1000
Access events	10	1000	1000	1000	1000
Alarm groups	74	138	138	138	138
Floor group	10	128	128	128	128
Door groups	10	128	128	128	128

Users

The database related to a user includes the following:

- User number (1 to 65,535)
- User name (16 characters)
- Alarm group (0 to 138)
- Door group (0 to 128)
- Floor group (1 to 64)
- PIN (4 to 10-digit sequence)
- Contact details
- Check boxes for *Card only, Extended access, Trace,* and *Privileged*
- Smart card options

The user database contains the following fields:

User number. The user number is a value between 1 and 65,535 and is used by the system to link a PIN or card to the functions it will do and the doors it can enter. When programming cards, the ID number programmed in the card is the user number (unless your system uses a card offset or intelligent user modules).

User numbers above 50 will only be accepted if a 1 MB, 4 MB, or 8 MB user memory module is used. User numbers above 11,466 will only accepted if a 4 MB or 8 MB user memory module is used.

User name. The user name is a text name with up to 40 characters (up to 20 characters for the first name and up to 20 characters for the last name). Only the first 200 names (50 if the system does not have memory expansion) and only the first 16 characters of each name will be downloaded.

Department. A department indicates the area that a user *works in*. Department details are entered in *Admin-Department*. Department details are only available for registered photo ID users.

User type. User types define the type of users for enhanced security and are only available in combination with a 4-door/elevator controller. User types include:

- Normal - Normal operation
- Two cards - Requires two valid user codes/cards to be presented to do any alarm or access control functions

- Guard - The user's code/card can only do functions when used in conjunction with a visitor's code/card.

PIN/card number. The PIN/card number holds the personal identification number for the user.

Confirm PIN/card number. The PIN/card number is hidden. To check that typing errors have not occurred, the number has to be typed in again in the *Confirm PIN/card number* box.

Users 1 to 1000 can have a PIN and/or card.

Users 1001 to 11,466 can only have a card, unless a software IUM is used. The PIN is created and is only valid when used with *Card and PIN* function on a 4-door/elevator controller.

All users can have a name in the software, however, only the first 200 names will be downloaded (50 if the system does not have any memory expansion).

Trace. All alarm and access functions done by the user will cause a trace message to be sent to the application software.

Card only. The user will not be able to use the PIN code. This allows the PIN code field to be used to program cards on formats not normally compatible with a special reader is used.

Privileged. The user's code/card will override any antipassback restrictions.

Extended access. The user will be allowed extended door unlock times.

Alarm group. The user's alarm group is used to assign alarm control and menu functions.

Door group. The user's door group determines through which doors and at what times the user can access the facility.

Floor group. The user's floor group determines through which floors and at what times the user can access the facility.

Comments. Add comments regarding the current user.

Card issue. When using card readers in combination with IUM modules or when smart cards are being programmed with a smart card programmer, the following card details can be edited.

- User number - The selected user number

- Card status - The current status of the card (active, disabled, void, reassigned, or lost).
- Raw card data - Shows a special number
- Credit issue - Adds credits to a user. Every user can have credits for up to four different accounts.
- Card security - Set the access level and the locations where the credits can be used.

Card read sequence

The typical card read operation is illustrated in the following steps:

- User 1 (facility code 100, card ID 5001) presents their card to a reader.
- The reader sends the card information to the control panel (facility code A: 100, B: 0 (not used), offset A: -5000, B: 0 (not used).
- The control panel queries the user database manager (User 1 record, name, PIN: 12345, user: 1).
- The databases returns the record of the card holder to the control panel and records the access event for User 1 in the event storage manager (event buffer, event access User 1).
- The control panel sends an *Access Granted* message to the reader.
- The reader notifies the user (beep, LED change, RTE) that access is granted.

Appendix C Text word library

By default, the system provides up to 900 predefined commonly used text words (referred to as the text word library). You can also define up to 100 additional text words to customize the library to your specific needs. The *Text words tool* on page 100 provides a searchable list of both predefined and user defined text words.

Text word library

A

Above	001	Area nine	340
Access	002	Area ten	341
Accountant	003	Area eleven	342
Accounts	264	Area twelve	343
Accounts manager	417	Area thirteen	344
Across	004	Area fourteen	345
Admin	404	Area fifteen	346
Administration	418	Area sixteen	347
Air conditioning	272	Armored car	410
Alarm	005	Arming	009
All	006	Art	421
All area user code	362	Assistant	265
All ATMs	520	Assistant manager	367
Amenities	419	Assistant manager day	369
Analog	295	Assistant principal	422
Ancillary staff	420	Assoc. administrator	423
And	514	At	010
APC	007	ATM	011
Area	008	Atrium	308
Area one	332	Audio	012
Area two	333	Auto	013
Area three	334	Auto arm	350
Area four	335	Auto disarm	351

Area five	336	Automatic	014
Area six	337	Auto reset	381
Area seven	338	Aux	015
Area eight	339	AV production	424

B

Back	016	Board	024
Baker	349	Boardroom	025
Baker 1	376	Body	026
Baker 2	377	Boiler	027
Bar	017	Bottom	028
Basement	018	Box	326
Bathroom	019	BRD	539
Battery	273	BRG	267
Bay	020	Building	029
Beam	021	Bulk store	425
Bedroom	022	Business	030
Bell	023	Button	031

C

Cabinet	032	Cleaner admin	413
Cage	033	Clerk	049
Call	034	Clip	050
Calibration	293	Cold	051
Camera	035	Combination	052
Canteen	036	Commerce	428
Car	037	Commercial	053
Caroline	038	Communication	054
Cash	039	Compactor	055
Cash office	408	Computer	056
CCTV	040	Computer room	429
Ceiling	041	Conference	057
Cellar	042	Conference room	430
Central	043	Contact	058
Central bulk store	426	Control	059
Center	431	Corridor	299
Charge	045	Count	358
Chief	046	Counter	060
Cigarettes	047	Cover	325
City	048	Covered area	432
Class room	427	Covering	061
Cleaner	352	Curtain	522
Cleaner selling	411	Custody	269
Cleaner front	412	Customer	062

D

Dairy	274	Door	069
Dark room	433	Door keypad	543
Data	304	Doors	465
Delayed	063	Double	503
Desk	266	DOTL	275
Detector	064	Downstairs	070
Developmental	434	Driveway	071
DGP	065	Drug	072
Dining	066	Dry craft	436
Digital	296	DUALTEK	074
Dispatch	067	Duct	073
District facility	435	Dump	330
Dock	068	Duress	075

E

Early	437	Enquiry	081
East	086	Entry	082
Education	438	Entry/display area	440
Electric	077	Equipment	083
Electrical	078	Equipment store	441
Electronics	439	Evaluation	298
Emergency	079	Exit	084
Engineering	297	Exterior	085
End	080	External	086

F

Factory	087	FLR	323
Factory manager	442	Foil	095
Fail	276	Food	277
Failure	088	Forced door	278
Fashion	089	Foyer	096
Fence	090	Freezer	097
File	091	Front	098
Film	092	Front counter	379
Fire	093	Front door keypad bank 1	538
Fitness testing	443	Front door keypad bank 2	542
Floor	094		

G

Games	099	Group 12	386
Gaming	283	Group 13	387
Gas	100	Group 14	388
Garden	101	Group 15	389
Garage	102	Group 16	390
Gate	103	Group 17	391
General	104	Group 18	392
General circulation	445	Group 19	393
General staff	530	Group 20	394
General staff 1	519	Group 21	395
General staff 2	532	Group 22	396
GLA	446	Group 23	397

GLA/stage	447	Group 24	398
Glass	105	Group 25	399
Goods	328	Group 26	400
Graphics	448	Group 27	401
Grd/Flr	312	Group 28	401
Groundsman store	449	Group 29	403
Ground	106	Guard	450
Group	303	Gun	279
Group 11	385	Gym	315

H

Hall	107	High SSO	527
Hallway	444	Holdup	110
Hand	108	Holdup bar	361
Hatch	327	Holdup button	382
Heat	109	Home economics	451
High level user master	364		

I

In	111	Instrument store	452
Inertia	280	Interior	113
Inner	281	Internal	114
Input	112	Isolate	524

J

K

L

M

Machine	134	Meat	329
Machine store	455	Mechanic	523
Magnetic	135	Medical	141
Main	136	Meeting	316
Main admin office	436	Mens	142
Main entry	457	Metal workshop	460
Mains	285	Microwave	143
Makash	318	Middle	144
Manager	137	Money	145
Manchester	138	Motion	146
Manual	458	Motor	147
Master	139	Multipurpose room	461
Master Advisor	044	Music	462
Mat	140	Music practice	463
Materials store	459	MYCP & interview	464

N

ND	313	Noise makers isolated	354
Near	148	North	152
New	268	North West	153
Next	149	North East	154
Next to	150	Note	155
Night	151	Number	156
Night manager	370		

O

P

Q

Quiet learning	478		

R

Rack	178	Representative	190
Radio	179	Reprographic production	480
Raid	180	Request to exit	518
Ramp	181	Research	264
RAS	317	Resource center	481
Reader	182	Resource store	482
Rear	183	Retrofit	300
Receiving	184	RF	306
Receiving dock	407	Right	191
Receiving door	378	Riser	309
Reception	185	Road	192
Record	186	Roller door	193
Reed switch	187	Roof	194
Reference	479	Room	195
Refrigeration	188	RSB	263
Register	307	Rumpus	196
Remote	189		

S

Siren	209	Store manager	366
Shutter	210	Store manager day	368
Sliding	211	Store room	331
Small	289	Storage	226
Small equipment store	489	Strobe	227
Small group	490	Strong room	359
Smoke	212	Strike	228
Sound	213	Student center	498
South	214	Student waiting	499
South East	215	Studies	500
South West	216	Studio	501
Spare	217	Substation	319
Special	491	Sump	291
Special access 1	414	Supermarket	229
Special access 2	415	Supervisor	230
Special access 3	416	Surveillance	231
Special education area	492	Switch	232
Sports store	493	Switchboard	292
Spray	494	System	233
Sprinkler	218		

T

Tamper	234	Textile store	509
Tape	235	The Challenger	044
Teacher	504	Time	238
Teacher work	505	To	239
Tea room	502	Toilet	240
Technical	301	Tool	241
Technician	506	Top	242
Telecom	320	Trading	271
Teller	236	Trades	510
Temp GLA	507	Transmitter	243
Temp typing	508	Trap	244
Temperature	237	Typing GLA	511

U

Ultrasonic	245	Upper	246
Under	512	Upstairs	247
Unit	513		

V

Valve	248	Ventilator	251
Vault	249	Video	252
Vault RAS bank 1	540	Voltage	253
Vault RAS bank 2	541	Volumetric	
Vent	250		

W

Wall	254	Wired grid	258
Warehouse	255	Women's	259
West	256	Wood workshop	516
Wet craft	515	Work room	517
Window	257	Workshop	260

Y

Yard	261		

Z

Zone	262		

Appendix D Numbering

This appendix provides an overview of Alliance system numbering.

In this appendix:

Numbering

Although Alliance Builder can handle the addressing/numbering for you, a basic knowledge of the numbering scheme will make programming the system and understanding the restrictions easier. Alliance systems can be very large and system components must be set-up to function together. The system addressing and numbering scheme is an essential element in this process.

It is important to understand the difference between addresses and numbers and how they relate to each other:

Addresses. Assigned to control panels, DGP devices, and RAS devices.

Numbers. Assigned to zones (inputs) and relays (outputs) on a device and are directly tied to the address of that device.

Each zone and relay is assigned a unique number. These numbers are grouped in blocks of 16 that are tied to a specific device address.

System bus

When mapping a system with DGP devices and expansion modules, you must know how many addresses are consumed by each component in the system. Systems with an AL-4017 or an AL-4617 control panel can support up to 16 addresses. Each address will consume up to 16 zone numbers for a total of up to 256 possible zones.

Zone numbers 1 through 16 are control panel zones because by default the control panel address is 0.

Table 49 shows the 16 system addresses and their related zones.

Table 49. Addresses and zones

Address	Zones
0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
1	17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32
2	33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48
3	49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64
4	65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80
5	81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96
6	97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112
7	113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128
8	129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144
9	145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160
10	161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176
11	177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192
12	193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208
13	209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224
14	225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240
15	241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256

Since the control panel consumes address 0, up to 15 addresses that can be used for DGP devices. By default each DGP device consumes a single DGP address. However, by expanding the number of zones a DGP device can control with a zone expansion module, a DGP device can consume zone numbers available in two addresses. Other DGP devices in the system can not use the second address or any of the 16 zone numbers assigned to the address.

Example 1

If the control panel on the system bus has an 8-zone expansion module, the control panel will consume the 16 zones in address 0 (zones 1 through 16) and the first 8 zones in address 1 (zones 17 through 24). In this instance, zones 25 through 32 will not be used by the control panel and will not be available for any other device. The dark gray shading in *Table 50* indicates the addresses and zones consumed by the control panel. The first address available for a DGP will be address 2.

Table 50. Example 1

Address	Zones
0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
1	17, 18, 19, 20, 21, 22, 23, 24,
2	33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48
3	49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64
4	65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80
5	81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96
6	97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112
7	113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128
8	129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144
9	145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160
10	161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176
11	177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192
12	193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208
13	209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224
14	225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240
15	241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256

Example 2

If a DGP with an 8-zone expansion module is added to the control panel, the DGP will consume the 16 zones in address 2 (zones 33 through 48) and the first 8 zones in address 3 (zones 49 through 56). Zones 57 through 64 will not be used by the DGP and will not be available for any other device. The dark gray shading in *Table 51* indicates the addresses and zones used by the control panel and light gray shading indicates the addresses and zones used by the first DGP. The next available address will be address 4.

Table 51. Example 2

Address	Zones
0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
1	17, 18, 19, 20, 21, 22, 23, 24
2	33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48
3	49, 50, 51, 52, 53, 54, 55, 56
4	65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80
5	81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96
6	97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112
7	113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128
8	129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144
9	145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160
10	161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176
11	177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192
12	193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208
13	209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224
14	225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240
15	241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256

Example 3

Although the system will support up to 15 DGP devices, the maximum number for your system will depend on the number of expansion modules you add to the control panel and DGP devices. If you add an expansion module to the control panel and to every DGP device on your system, the system will only support 7 DGP devices. As shown in *Table 52*, the control panel will consume addresses 0/1 and the 7 DGP devices will consume addresses 2/3, 4/5, 6/7, 8/9, 10/11, 12/13, and 14/15. This in turn will limit the actual number of zones/relays available for your system. Any of the 16 zone numbers assigned to an address that are not used by the device consuming that address are not available for use by any other device.

Table 52. Example 3

Address	Zones
0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
1	17, 18, 19, 20, 21, 22, 23, 24
2	33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48
3	49, 50, 51, 52, 53, 54, 55, 56
4	65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80
5	81, 82, 83, 84, 85, 86, 87, 88
6	97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112
7	113, 114, 115, 116, 117, 118, 119, 120
8	129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144
9	145, 146, 147, 148, 149, 150, 151, 152
10	161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176
11	177, 178, 179, 180, 181, 182, 183, 184
12	193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208
13	209, 210, 211, 212, 213, 214, 215, 216
14	225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240
15	241, 242, 243, 244, 245, 246, 247, 248

4-door/elevator controller

A maximum of 48 doors are supported by the Alliance system. This means that although you can have up to 15 DGP devices of different types combined on the system bus, only 12 of the devices can be 4-door/elevator controllers. *Table 53* shows the door numbers, zones, and relays that would be associated with each 4-door/elevator controller address on the system bus.

Table 53. 4-door/elevator controller addresses

DGP address	Door numbers	Zones (inputs)	Relays (outputs)
1	17 - 20	17 - 32	17 - 32
2	21 - 24	33 - 48	33 - 48
3	25 - 28	49 - 64	49 - 64
4	29 - 32	65 - 80	65 - 80
5	33 - 36	81 - 96	81 - 96
6	37 - 40	97 - 112	97 - 112
7	41 - 44	113 - 128	113 - 128
8	45 - 48	129 - 144	129 - 144
9	49 - 52	145 - 160	145 - 160
10	53 - 56	161 - 178	161 - 178
11	57 - 60	179 - 192	179 - 192
12	61 - 64	193 - 208	193 - 208

Zone and relay mapping

When a 4-door/elevator controller is assigned a DGP address on the system bus, it automatically calculates its default zone and relay numbers. The controller has four onboard relays that by default are designated as unlock relays. Only numbers associated with the DGP address can be assigned to these zone and relay functions. These 4-door/elevator controller relay assignments only activate relays connected to it. If zones are disabled, they revert to being normal DGP system zones. Any zones assigned as door contact zones or DOTL zones also have to be assigned a zone type in Zone programming. The zone type assigned defines how the system responds to alarms on these zones.

Relays and expansion

When adding a relay expansion module to the 4-door/elevator controller, it is important that the 4-door/elevator controller be programmed for relay expansion modules when the module is clocked and not enabled when the relay expansion module is not clocked. You cannot install both clocked and non-clocked modules on the same 4-door/elevator controller.

For example, the AL-1810 is a four relay expansion module that is not clocked. When this unit is installed on a 4-door controller, the controller should not have the relay expansion modules programmed. This configuration provides four additional relays in addition to the four on board relays of the controller. This configuration is physically relay one through eight with the first four actually on the controller. If the relay expansion module is enabled through the 4-door controller programming, it will not function properly and will continuously cycle the relays with noticeable chatter.

When installing a clocked relay expansion module, the controller must be programmed with the number of relays installed. In the case of an AL-1813 8-relay expansion module, the physical relays will map over the controllers four on board relays. Any action that can cause the relay to become active will duplicate on the first four relays. For example, if the controllers on board relay 1 becomes active, then relay 1 on the AL-1813 also becomes active.

Door/card reader numbering

The 4-door/elevator controller has card reader input capabilities, with a maximum of 16 readers. Each of the four doors can have up to four card readers. Of these four readers, two will be in readers and two will be out readers. *Table 54*shows the readers associated with each door. Notice that the reader numbers for each door are not sequential. For example, Door 1 has reader numbers 1, 5, 9, and 13.

Table 54. Door/card reader numbering

Door number	IN reader	IN reader	OUT reader	OUT reader
1st Door	1	5	9	13
2nd Door	2	6	10	14
3rd Door	3	7	11	15
4th Door	4	8	12	16

RAS numbering

Relay (output) control group numbering

Relay control group numbers are a way to identify a group of 8 relays (outputs) controlled by a RAS device. When a relay control group is assigned to a RAS device, the open collector relay (OUT) terminal, follows the first relay of the relay control group.

Table 55 illustrates the relay control group numbering details:

Table 55. Relay control group numbering

Group	Relay number		Group	Relay number
1	1		17	129
2	9		18	137
3	17		19	145
4	25		20	153
5	33		21	161
6	41		22	169
7	49		23	177
8	57		24	185
9	65		25	193
10	73		26	201
11	81		27	209
12	89		28	217
13	97		29	225
14	105		30	233
15	113		31	241
16	121		32	249

Appendix E Zone event reporting

This appendix provides a table of the reported zone event per sub-class and condition.

Zone event reporting

Table 56 shows the reported zone event per sub-class and condition. The CID column holds the reported Contact ID event, the SIA column holds the SIA event.

Zone event type numbers 1 to 12 and 43 to 49 are not in the table and should not be used.

Table 56. Zone event reporting

Type number	Class	Sub-class	Condition	CID	SIA
13	Panic	Panic 120 (PA)	Alarm	E120	PA
			Tamper	E383	TA
			Bypass	E570	PB
			Alarm restore	R120	PR
			Tamper restore	R383	TR
			Bypass restore	R570	PU
14	Panic	Panic 121 (HA) duress	Alarm	E121	HA
			Tamper	E83	TA
			Bypass	E570	HB
			Alarm restore	R121	HR
			Tamper restore	R383	TR
			Bypass restore	R570	HU
15	Panic	Panic 122 (PA) silent panic	Alarm	E122	PA
			Tamper	E383	TA
			Bypass	E570	PB
			Alarm restore	R122	PR
			Tamper restore	R383	TR
			Bypass restore	R570	PU

Table 56. Zone event reporting (continued)

Type number	Class	Sub-class	Condition	CID	SIA
16	Panic	Panic 123 (PA) audible panic	Alarm	E123	PA
			Tamper	E383	TA
			Bypass	E570	PB
			Alarm restore	R123	PR
			Tamper restore	R383	TR
			Bypass restore	R570	PU
17	Burglar	Burglar 130 (BA) burglary	Alarm	E130	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R130	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU
18	Burglar	Burglar 131 (BA) perimeter	Alarm	E131	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R131	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU
19	Burglar	Burglar 132 (BA) interior	Alarm	E132	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R132	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU

Table 56. Zone event reporting (continued)

Type number	Class	Sub-class	Condition	CID	SIA
20	Burglar	Burglar 133 (BA) 24-hour	Alarm	E133	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R133	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU
21	Burglar	Burglar 134 (BA) entry/exit	Alarm	E134	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R134	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU
22	Burglar	Burglar 135 (BA) day/night	Alarm	E135	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R135	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU
23	Burglar	Burglar 136 (BA) outdoor	Alarm	E136	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R136	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU

Table 56. Zone event reporting (continued)

Type number	Class	Sub-class	Condition	CID	SIA
24	Burglar	Burglar 137 (BA) tamper	Alarm	E137	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R137	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU
25	Burglar	Burglar 138 (BA) near alarm	Alarm	E138	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R138	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU
26	General alarm	General 140 (UA) general alarm	Alarm	E140	UA
			Tamper	E383	TA
			Bypass	E570	UB
			Alarm restore	R140	UR
			Tamper restore	R383	TR
			Bypass restore	R570	UU
27	General alarm	General 141 (UA) polling loop open	Alarm	E141	GA
			Tamper	E383	TA
			Bypass	E570	GB
			Alarm restore	R141	GR
			Tamper restore	R383	TR
			Bypass restore	R570	GU

Table 56. Zone event reporting (continued)

Type number	Class	Sub-class	Condition	CID	SIA
28	General alarm	General 142 (UA) polling loop short	Alarm	E142	ZA
			Tamper	E383	TA
			Bypass	E570	ZB
			Alarm restore	R142	ZR
			Tamper restore	R383	TR
			Bypass restore	R570	ZU
29	General alarm	General 143 (ET) exp. module fail	Alarm	E143	SA
			Tamper	E383	TA
			Bypass	E570	SB
			Alarm restore	R143	SR
			Tamper restore	R383	TR
			Bypass restore	R570	SU
30	General alarm	General 144 (TA) sensor tamper	Alarm	E144	WA
			Tamper	E383	TA
			Bypass	E570	WB
			Alarm restore	R144	WR
			Tamper restore	R383	TR
			Bypass restore	R570	WU
31	General alarm	General 145 (TA) exp. module tamper	Alarm	E145	BA
			Tamper	E383	TA
			Bypass	E570	BB
			Alarm restore	R145	BR
			Tamper restore	R383	TR
			Bypass restore	R570	BU

Table 56. Zone event reporting (continued)

Type number	Class	Sub-class	Condition	CID	SIA
32	24-hour alarms	24-hour 150 (UA) 24-hour nonburg	Alarm	E150	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R150	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU
33	24-hour alarms	24-hour 151 (GA) gas detected	Alarm	E151	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R151	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU
34	24-hour alarms	24-hour 152 (ZA) refrigeration	Alarm	E152	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R152	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU
35	24-hour alarms	24-hour 153 (ZA) loss of heat	Alarm	E153	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R153	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU

Table 56. Zone event reporting (continued)

Type number	Class	Sub-class	Condition	CID	SIA
36	24-hour alarms	24-hour 154 (WA) water leakage	Alarm	E154	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R154	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU
37	24-hour alarms	24-hour 155 (QA) foil break	Alarm	E155	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R155	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU
38	24-hour alarms	24-hour 156 (UA) day trouble	Alarm	E156	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R156	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU
39	24-hour alarms	24-hour 157 (ZA) low bottled gas level	Alarm	E157	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R157	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU

Table 56. Zone event reporting (continued)

Type number	Class	Sub-class	Condition	CID	SIA
40	24-hour alarms	24-hour 158 (ZA) low temperature	Alarm	E158	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R158	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU
41	24-hour alarms	24-hour 159 (ZA) low temperature	Alarm	E159	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R159	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU
42	24-hour alarms	24-hour 161 (ZA) loss of air flow	Alarm	E161	QA
			Tamper	E383	TA
			Bypass	E570	QB
			Alarm restore	R161	QR
			Tamper restore	R383	TR
			Bypass restore	R570	QU

Appendix F Zone types

This appendix provides a table of zone types.

Zone types

Table 57 shows the zone types by number, name and description.

Table 57. Zone types

Number and name	Description
0. Disabled	No alarms are generated by this zone. **Disarmed flags:** none **Armed flags:** none
1. Disarmed alarm	Generates an alarm when the area is disarmed and reports it to the central station. Does not generate an alarm if the area is armed. *Example:* Panic alarm button **Disarmed flags:** disarmed alarm, 24 hour, zone flag **Armed flags**: none
2. Armed alarm	Generates an alarm when the area is armed. Does not generate an alarm when the area is disarmed. *Example:* Internal door, PIR (motion detector) **Disarmed flags**: none **Armed flags**: siren, armed alarm, 24-hr., zone flag
3. Entry/exit alarm	Does not generate an alarm when the area is disarmed. When the area is armed, the exit timer starts and activating the zone will not generate an alarm. If the zone is activated and the exit time has expired, the entry timer starts. When the entry time has expired, an alarm will be generated. The zone must be closed when arming the area. *Example:* Final exit door **Programming:** Program the *entry/exit time* in *Area programming, and enable the buzzers* in *RAS programming*. **Disarmed flags:** none **Armed flags**: siren, armed alarm 24-hr., zone flag

Table 57. Zone types (continued)

Number and name	Description
4. Access zone	Generates an alarm when the area is armed. Does not generate an alarm when the area is disarmed. The zone is bypassed during the entry/exit timed periods. The zone must be closed when arming the area. *Example:* PIR within the area's designated entry/exit route **Programming:** Program the *entry/exit time* in *Area programming* and *enable the buzzers* in *RAS programming*. **Disarmed flags:** none **Armed flags:** siren, armed alarm, 24-hr., zone flag
5. 24-hour alarm	Generates an alarm regardless of the status of the area. *Example*: Tampers, panic alarm buttons **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
6. Pulsed keyswitch	When the zone switches from normal state to active, the functions of the programmed alarm group are performed. The arming and disarming operation is dependent on the options programmed in the selected alarm group. Disarm only, arm and reset only, or alarm reset only may be selected. *Example*: Keyswitch to arm/disarm areas **Programming:** Program the required option in *Alarm groups programming*. Allocate this alarm group number to the zone in *Zone programming*. **Disarmed flags:** none **Armed flags:** none
7. Camera suspicion	When this zone is activated, cameras in the areas assigned to the zone will be activated. When the zone deactivates, the cameras continue to operate for the selected suspicion time. *Example:* Suspicion button **Programming:** Program the *suspicion time* in *Timers programming*. **Disarmed flags**: none **Armed flags:** none

Table 57. Zone types (continued)

Number and name	Description
8. Disarmed delayed/armed general alarm	Generates an alarm when the area is disarmed, but does not report it until the delayed alarm timer has expired or a second delayed alarm is activated. *Example:* Delayed panic alarm button (pressing a second delayed panic alarm button will override the delay) **Programming:** Program the *delayed disarmed alarm time* in *Timers programming*. **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
9. Reset delayed	Resets a delayed alarm type if the zone pulses to active and returns to its normal state. Reset a delayed alarm type if the delay timer is running and a full alarm has not occurred. Stops cameras from operating if the zone is activated, but the delayed time continues to run. Delayed zone types are 8, 11, 22, and 40. *Example: R*eset button for quick cancellation of the delayed alarm **Disarmed flags**: none **Armed flags:** none
10. Do not use	
11. Disarmed delayed alarm	Generates an alarm when the area is disarmed, but does not report it to the central station until the delayed alarm timer has expired or a second delayed alarm has activated. Does not generate an alarm if the area is armed. *Example:* Delayed panic alarm button **Programming:** Program the *delayed disarmed alarm time* in *Timers programming*. **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** none
12. Restart exit timer	A pulsed keyswitch that resets the entry timers and restarts the exit timers for all areas assigned to the zone. *Example:* Keyswitch near the final exit door **Disarmed flags:** none **Armed flags:** none

Table 57. Zone types (continued)

Number and name	Description
13. Entry/exit without arm check	Does not generate an alarm when the area is disarmed. When the area is armed, the exit timer starts, and activating the zone will not generate an alarm. If the entry time has expired, an alarm will be generated. The zone may be active while arming the area. *Example:* Final exit door **Programming:** Program the *entry/exit time* in *Area programming* and *enable the buzzers* in *RAS programming*. **Disarmed flags:** none **Armed flags:** siren, armed alarm, 24-hr., zone flag
14. Access without arm check	Does not generate an alarm when the area is disarmed. Generates an alarm when the area is armed. Bypassed during entry/exit timed periods. *Example:* PIR within the area's designated entry/exit route **Programming:** Program the *entry/exit time* in *Area programming* and *enable the buzzers* in *RAS programming*. **Disarmed flags:** none **Armed flags:** siren, armed alarm, 24-hr., zone flag
15. Emergency door	Generates a local alarm when the area is disarmed. Automatically activates an audible alert on the RAS assigned to the same areas (regardless of the event flag programming). The only event flag activated (as specified in Zone Programming) is the zone flag. If the zone reactivates it generates a new local alarm after the local alarm reminder time. *Example:* Emergency door **Programming:** Program the *local alarm reminder time* in *Timers programming*. **Disarmed flags:** zone flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
16. Do not use	
17. Do not use	
18. 24-hour local comms fail	Generates a local alarm. Activates an audible alert on all RAS assigned to the same areas. Activates the fault LED on all RAS. **Disarmed flags:** zone flag **Armed flags:** none

Table 57. Zone types (continued)

Number and name	Description
19. Comms fail LED	Activates the fault LED on all RAS. **Disarmed flags:** none **Armed flags:** none
20. Zone to event flag 24-hour	When the zone is activated, opened, or shorted, the zone event flag is activated. *Example:* Doorbell **Disarmed flags:** zone flag **Armed flags:** zone flag
21. Emergency door with a user code	Generates a local alarm when the area is disarmed, but does not report it to the central station. Generates an alarm when the area is armed. *Example:* Emergency door **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren armed alarm
22. Disarmed delayed with autoreset/ armed alarm	Generates an alarm when the area is disarmed, but does not report to the central station until the delayed alarm timer has expired or a second delayed alarm is activated. If the zone closes to normal state during the delayed time, it resets automatically. Generates an alarm when the area is armed. *Example:* Delayed panic alarm button (pressing a second panic alarm button will override the delay) **Programming:** Program the *delayed disarmed alarm time* in *Timers programming*. **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
23. Camera 1 count	Used to increment the film counter for camera 1 by connecting a normally open contact across the zone. The counter increments if the zone switches from open to short. This zone can only be used on the Alliance control panel. **Disarmed flags:** none **Armed flags:** none

Table 57. Zone types (continued)

Number and name	Description
24. Camera 2 count	Used to increment the film counter for camera 2 by connecting a normally open contact across the zone. The counter increments if the zone switches from open to short. This zone can only be used on the Alliance control panel. **Disarmed flags:** none **Armed flags:** none
25. Camera 3 count	Used to increment the film counter for camera 3 by connecting a normally open contact across the zone. The counter increments if the zone switches from open to short. This zone can only be used on the Alliance control panel. **Disarmed flags:** none **Armed flags:** none
26. Camera 4 count	Used to increment the film counter for camera 4 by connecting a normally open contact across the zone. The counter increments if the zone switches from open to short. This zone can only be used on the Alliance control panel. **Disarmed flags:** none **Armed flags:** none
27. Technical with report	When the zone is activated, opened, or shorted, it reports to the central station. A restore is sent when the zone returns to its normal state. *Example:* Temperature alarm on a freezer **Disarmed flags:** zone flag **Armed flags:** zone flag
28. Armed alarm with autoreset	Does not generate an alarm when the area is disarmed. Generates an alarm when the area is armed. Resets automatically when the zone returns to its normal state. *Example:* Latching glassbreak detector **Disarmed flags:** none **Armed flags:** siren, armed alarm, 24-hr., zone flag

Table 57. Zone types (continued)

Number and name	Description
29. 24-hour alarm with autoreset	Generates an alarm regardless of the status of the area. Resets automatically when the zone returns to its normal state. *Example:* Latching glassbreak detector **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
30. Emergency door with autoreset	Generates a local alarm when the area is disarmed, but does not report it to the central station. Resets automatically when the zone returns to its normal state. *Example:* Emergency door **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
31. Latching keyswitch	Used to arm or disarm areas. When the zone switches to an active state, the areas arm. Switching the zone to its normal state disarms the area. This zone type uses an alarm group to perform the arm/disarm functions. Program the required options in Alarm Group Programming and allocate this alarm group number to the zone. **Disarmed flags:** none **Armed flags:** none
32. Armed zone to an event flag	When the area is armed, and the zone is activated, opened, or shorted, the zone event flag is activated. Does not perform any action when the area is disarmed. *Example:* Temperature alarm on a freezer that activates an audible warning. **Disarmed flags:** none **Armed flags:** zone flag

Table 57. Zone types (continued)

Number and name	Description
33. 24-hour alarm and bypass	This zone requires different wiring and can have the following states: Shorted - Generates an alarm Normal - No alarm Active - Bypassed (no alarm generated) Open - Tamper alarm *Example:* Keyswitch to bypass a zone (designed for shopping centers where only one zone is available for each shop) **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
34. Area disarmed/alarm group restriction armed	A latching keyswitch that has special functions. Switching from normal state to active starts the warning time for the alarm group restriction assigned to the alarm group. When the warning time expires, the area arms. Switching from active to normal state disarms the area. **Programming:** Program an alarm group with an alarm group restriction enabled and allocate this alarm group number to the zone. Program the *timed disarmed areas* for this zone and complete the other options in *Alarm group restriction programming*. Program the *warning time* in *Timers programming*. **Disarmed flags:** none **Armed flags:** none
35. Area alarm group restriction armed only	A latching keyswitch that has special functions. Switching from normal state to active starts the warning time for the alarm group restriction assigned to the alarm group. When the warning time expires, the area arms. Switching from active to normal state does not perform any action. *Example:* Arming keyswitch in a large building that indicates that the area is going to arm **Programming:** Program an alarm group with an alarm group restriction enabled and allocate this alarm group number to the zone. Program the *timed disarmed areas* for this zone and complete the other options in *Alarm group restriction programming*. **Disarmed flags:** none **Armed flags:** none

Table 57. Zone types (continued)

Number and name	Description
36. Camera 5 count	Used to increment the film counter for camera 5 by connecting a normally open contact across the zone. The counter increments if the zone switches from open to short. This zone can only be used on the Alliance control panel. **Disarmed flags:** none **Armed flags:** none
37. Camera 6 count	Used to increment the film counter for camera 6 by connecting a normally open contact across the zone. The counter increments if the zone switches from open to short. This zone can only be used on the Alliance control panel. **Disarmed flags:** none **Armed flags:** none
38. Camera 7 count	Used to increment the film counter for camera 7 by connecting a normally open contact across the zone. The counter increments if the zone switches from open to short. This zone can only be used on the Alliance control panel. **Disarmed flags:** none **Armed flags:** none
39. Camera 8 count	Used to increment the film counter for camera 8 by connecting a normally open contact across the zone. The counter increments if the zone switches from open to short. This zone can only be used on the Alliance control panel. **Disarmed flags:** none **Armed flags:** none

Table 57. Zone types (continued)

Number and name	Description
40. Disarmed suspicion delayed/armed alarm	If the area is disarmed it has the following functions: Shorted - Activates cameras in the areas that are assigned to the zone. When the zone switches back to normal, the cameras continue to operate for the suspicion time. Normal - No alarm Active - Generates an alarm, but does not report to the central station until the delayed alarm timer has expired or a second delayed alarm is activated. Open - Tamper alarm Generates a general burglar alarm when the area is armed. **Programming:** Program the *delayed disarmed alarm time* in timers programming. **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
41. Entry/exit emergency door	Generates a local alarm when the area is disarmed. Automatically activates an audible warning on the RAS assigned to the same areas (regardless of the event flag programming). The only event flag activated is the zone flag. If the zone reactivates, it will generate a new local alarm after the programmed local alarm reminder time. When the area is armed, the exit timer starts and activating the zone will not generate an alarm. If the area is armed and the zone is activated, the entry timer will start. When the entry time has expired, an alarm will be generated. The zone must be closed when arming the area. *Example:* Emergency door that is also used to enter the premises **Programming:** Program the *entry/exit time* in *Area programming* and *enable the buzzers* in *RAS programming*. Program the *local alarm reminder time* in *Timers programming*. **Disarmed flags:** zone flag **Armed flags:** siren, armed alarm, 24-hr., zone flag

Table 57. Zone types (continued)

Number and name	Description
42. Entry/exit emergency door with code	Generates a local alarm when the area is disarmed, but does not report it to the central station. When the area is armed, the exit timer starts and activating the zone will not generate an alarm. if the area is armed and the zone is activated, the entry timer starts. When the entry time has expired, an alarm is generated. *Example:* Emergency door that is also used to enter the premises **Programming:** Program the *entry/exit time* in *Area programming* and *enable the buzzers* in *RAS programming*. **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
43. Disarmed zone to event flag	When the area is disarmed, and the zone is activated, opened, or shorted, the zone event flag is activated. When the area is armed, no action is taken. *Example:* Opening a cupboard activates an audible warning **Disarmed flags:** zone flag **Armed flags:** none
44. Emergency door with alarm group restriction	Generates a local alarm when the area is disarmed, but does not report it to the central station. Generates an alarm when the area is armed. The zone can be disabled when two users with alarm group restrictions enter their user code (not necessarily in the same area). *Example:* Emergency door **Programming:** Program an alarm group and an alarm group restriction. **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
45. (Event flag/armed alarm) alarm group restriction	Activates the zone event flag when the area is disarmed. Generates an alarm when the area is armed. The zone can be disabled if two users with alarm group restrictions enter their user codes (not necessarily in the same area). **Programming:** Program an alarm group and an alarm group restriction. **Disarmed flags:** zone flag **Armed flags:** siren, armed alarm, 24-hr., zone flag

Table 57. Zone types (continued)

Number and name	Description
46. Disarmed alarm/armed general alarm	Generates an alarm if the area is disarmed. Generates a general burglar alarm if the area is armed. **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
47. Disarm alarm suspicion/ armed general alarm	While disarmed the generation of an alarm activates the cameras. When the zone closes to its normal state, the cameras continue to operate for the suspicion time. Generates a general alarm if the area is armed. **Disarmed flags**: disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
48. Camera 1 film out	Generates an alarm when camera 1 is out of film. **Disarmed flags:** zone flag **Armed flags:** zone flag
49. Camera 2 film out	Generates an alarm when camera 2 is out of film. **Disarmed flags:** zone flag **Armed flags:** zone flag
50. Camera 3 film out	Generates an alarm when camera 3 is out of film. **Disarmed flags:** zone flag **Armed flags:** zone flag
51. Camera 4 film out	Generates an alarm when camera 4 is out of film. **Disarmed flags:** zone flag **Armed flags:** zone flag
52. Camera 5 film out	Generates an alarm when camera 5 is out of film. **Disarmed flags:** zone flag **Armed flags:** zone flag
53. Camera 6 film out	Generates an alarm when camera 6 is out of film. **Disarmed flags:** zone flag **Armed flags:** zone flag
54. Camera 7 film out	Generates an alarm when camera 7 is out of film. **Disarmed flags:** zone flag **Armed flags:** zone flag

Table 57. Zone types (continued)

Number and name	Description
55. Camera 8 film out	Generates an alarm when camera 8 is out of film. **Disarmed flags:** zone flag **Armed flags:** zone flag
56. Emergency door if no time zone 41	If time zone 41 is invalid, the zone generates a local alarm when the area is disarmed but does not report it to the central station. Generates an alarm when the area is armed. If time zone 41 is valid, the zone is disabled. Unless inverted, when the output is activated, the time zone is valid. *Example:* Emergency door **Programming:** Program the *local alarm reminder time* in *Timers programming* and link time zone 41 to an output (relay) in *time zone to follow an output*. **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
57. Technical report and screen	When the zone is activated or tampered, it reports to the central station and puts the zone event text on the display. A remote is sent when the zone switches to its normal state. *Example:* Temperature alarm on a freezer **Programming:** Program the *zone event text word* in *System options programming*. **Disarmed flags**: zone flag **Armed flags:** zone flag
58. Technical screen	When the zone is activated, opened, or shorted, it puts the zone event text on the display. *Example:* Temperature alarm on a freezer **Programming:** Program the *zone event text word* in *System options programming*. **Disarmed flags:** zone flag **Armed flags:** zone flag

Table 57. Zone types (continued)

Number and name	Description
59. 24-hour alarm if no time zone 41	If time zone 41 is invalid the zone generates an alarm regardless of the status of the area. If time zone 41 is valid, the zone is disabled. Unless inverted when the output is activated, the time zone is valid. **Disarmed flags:** disarmed alarm, 24-hr., zone flag, camera flag **Armed flags:** siren, armed alarm, 24-hr., zone flag
60. Exit terminator	This zone type is used to terminate the exit time. If the zone switches from active to normal, the exit time is terminated and the areas are completely armed. **Disarmed flags:** none **Armed flags:** none
61. Do not use	
62. Do not use	
63. Do not use	
64. Do not use	
65. Engineer reset	This zone type is used to perform an engineer reset. When active, an engineer reset will be performed on the area assigned to the zone. **Disarmed flags**: none **Armed flags**: none
66. Final door set	This zone type is used to shorten the exit timer when the sensor associated with this zone is activated (normally on an exit door). When activated, it shortens the exit timer to 4 seconds. If not needed, set the exit time to 0.
67. Latched detector	This zone type has a 24-hour alarm that can be isolated and associated with a latched detector event flag.
68. Antimask detector	This zone type is the same as zone type 2 (*Armed alarm*). It gives a special indication for remote diagnostics purposes.

Table 57. Zone types (continued)

Number and name	Description
69. Alarm (APCO) zone	Does not generate an alarm when the area is disarmed. Generates an alarm when the area is armed. Bypassed during the entry/exit timed periods. The zone must be closed when arming the areas. **Disarmed flags**: none **Armed flags:** siren, armed alarm, 24-hr., zone flag
70. Keybox	This zone type is linked to the keybox timer. It has a 24-hour alarm. When the keybox zone is active (keybox door/lid will not be opened during exit or keybox timer) it reports an alarm to the ARC.

Glossary

This section explains some terms as they apply to Alliance Builder.

Table 58. Alliance Builder terms explained

Term	Definition
Access control	The control of entry to, or exit from, a security area.
Active	When used in relation to a zone (input) device, the zone device is activated. For example, an emergency exit door is open.
Alarm	The state of a security system when an armed zone device is activated. For example, a PIR device has detected an intruder causing a siren to sound.
Alarm control	The control of alarm functions.
Alarm group	Alarm groups are assigned to users, RAS devices, or door readers to define what areas can be controlled and what functions can be done by that user, from that device, and during what times. An alarm group can also be assigned to certain zone types.
Alarm group restriction	An alarm group restriction can be assigned to an alarm group to enable different types of users to use the timed disarmed function on certain areas, restrict alarm control to arm/reset only on certain areas, or to use the user count or emergency functions.
Alarm reporting	A procedure to transmit alarm or other events to a central station by means of a dialer and a set of rules called a protocol.
Area	A section of a building that has specific security requirements. The control panel allows a building to be divided into 16 areas of differing security requirements. Each area is identified with a number and a name.
Armed	The condition of a zone, an area, or a building when a change of the status of any zone will cause an alarm. An area or building is armed only when it is unoccupied, while some zones may remain armed continually.
Arming station	Also referred to as RAS devices, arming stations can be LCD keypads, readers, or any other device that can be used to perform security functions such as arming, disarming or opening doors.

Table 58. Alliance Builder terms explained (continued)

Term	Definition
Badge	A badge identifies a person to the Alliance system. A badge typically has a unique identity number consisting of a badge number and site code. The term badge also applies to a PIN because a badge does not have to be a physical device, it can be a PIN only. See Card.
Battery	Back-up power to prevent system failure in case of AC power trouble.
Battery test	Periodic test of the battery to ensure proper functioning.
Bypassed	A zone input has been excluded from functioning as part of the system and does not indicate normal or active status.
Card	A card identifies a person to the Alliance system. A card typically has a unique identity number consisting of a card number and site code. See Badge.
Card active	An active card can be used to gain access to doors or floors provided the door group allows access.
Card disabled	A disabled card can not be used to gain access to doors or floors
Central station	A central station is a company that monitors whether an alarm has occurred in a security system. A central station is located away from the building/area it monitors.
Cloning	Cloning is used to make an exact copy of an existing system.
Control panel	A control panel is an electronic device that is used to gather all data from zone inputs on the premises. Depending on programming and status of areas, the control panel generates alarm signals and reports alarms and other events to a central station.
DGP	(Data Gathering Panel) A device that collects data from other security devices within an area, and transfers it to the main control panel or 4-door controller.
Dialer	A dialer is an electronic device that allows the system to transmit alarms and other events to a central station. It can also perform up and downloads.
Disarmed	When the security system has been programmed so that normal activity does not set off an alarm, the condition of the area or building is referred to as disarmed.
Door contact	A door contact is a magnetic contact used to detect if a door or window is opened.
Door control	Door control is the control over door functions.

Table 58. Alliance Builder terms explained (continued)

Term	Definition
Door group	A door group assigns a group of doors to a user, in order to allow the user access to those doors. Access to each door in a group can be restricted via a time zone.
Download	Download is a method to send information to control panels.
Duress	When a user is being forced to breach the security system, it is considered a duress situation. The system's duress feature allows the user to signal a central station that a duress situation is occurring by entering a duress digit in conjunction with a PIN code.
Enable/disable doors	By default a door is enabled. When a card is badged on a reader associated with the door, the door will open. When disabled, the reader will not react to a card being badged and the door will not open.
Event flags	Event flags are signals activated by a zone input condition, area condition, system status or fault condition. The main purpose of an event flag is to activate an output.
Event to output	Event to output creates links between event flags and outputs. Outputs are available as relays or as open collector outputs.
Facility	A facility is a grouping of database records typically used to indicate a building, location, or function.
Forced arm	Forced arming is arming with automatic bypass on any zone that is active.
Hard time zone	Hard time zones are clocked-based and are valid between programmed start and end times. Hard time zones are allocated to control panel functions to control the activity of that function by time and day and are primarily used to restrict access or to automatically arm/disarm areas.
History	History, in this instance, refers to a list of past alarm and access control events stored in memory that can be viewed on an LCD arming station (RAS) or sent to a printer.
Hold-up	Hold-up refers to a silent alarm triggered by a hold-up button. Normally it will not trigger a siren, only send a message to a central station.
Installer	Installer refers to the company that installs and services security equipment.
IUM memory	Intelligent User Module - A 4 or 8 MB memory expansion module for a control panel and associated with intelligent DGPs (data gathering panels).

Table 58. Alliance Builder terms explained (continued)

Term	Definition
Keypad	A keypad is a RAS (remote arming station) with keys to input data used to program the control panel, perform user functions, and view alarms.
Keyswitch	A keyswitch is a device using a switch with a key to arm or disarm areas.
LCD	(Liquid Crystal Display) This is the part of a RAS (remote arming station) where messages or programming details are displayed.
LED	(Light Emitting Diode) This is a light indicator on a RAS (remote arming station), which indicates a condition.
Local alarm	A local alarm is transmitted only within a building and occurs when an area is occupied. The circumstances which cause a local alarm can be checked and rectified by personnel on site and it is therefore unnecessary for the alarm to be transmitted to a central station.
Local bus	The local bus connects devices (both RAS and DGPs) to a 4-Door Controller DGP. These devices are not visible to the control panel.
Lock/unlock doors	A door can be locked or unlocked. Unlocking a door will open the door until locked again by a lock command, either from the software program or an event that will lock the door.
Log off	Logging off prohibits the use of the software program.
Log on	Logging on is required before the software program can be used. Enter your operator name and password to log on.
Logic equation	A logic expression that combines macro inputs in a specific manner. The result of a logic equation is called a macro output.
Macro input	Each macro input is an event flag or output that is used in a logic equation.
Macro logic program	A macro logic program is a set of rules that is created by macro inputs, logic equations, and macro outputs that is used to trigger event flags or zone inputs.
Macro output	A macro output is the result of a logic equation. The macro output can have a timing element and trigger event flags or zone inputs.
Normal	When used in relation to a zone device, the zone device is normal when it is not activated.
Online/offline	Operational/Non-operational - A device may be offline due to a malfunction in the device itself or it may be disconnected from the control panel.

Table 58. Alliance Builder terms explained (continued)

Term	Definition
Output	Outputs provide physical contacts that can be used to activate LEDs, relays, etc. An output can have two states: active, or not active.
Output control	A PCB module that connects to the control panel or a DGP (data gathering panel) to provide relay or open collector outputs. When programming, 1 output controller equals 8 outputs.
PIN	A PIN code is a 4 to 10-digit number given to, or selected by, a user. It is necessary to enter a PIN code on an Alliance keypad as a prerequisite to perform most functions. in programming, the PIN code is associated with a user number, which identifies the PIN code holder to the system.
PIR detector	Passive Infrared detector - This security device is used to detect intruders in a certain part of an area or premise using infrared detection.
Poll	A poll is an inquiry message continually sent by the control panel to DGPs (data gathering panels) and RAS (remote arming stations). Polling allows the remote unit to transfer data to the control panel.
RAS	(Remote Arming Station) A RAS is the user's control panel for security functions for areas or for access points (doors). The RAS can be a console (LCD keypad, reader) or any other device that can be used to perform security functions such as arm/disarm, open doors, etc.
Reader	A reader is a device used for access control that can read cards to allow access. Depending on the needs and the type of cards, the reader can be a magnetic swipe reader or a proximity reader.
RTE zone	(Request-to-Exit) zone - This is a zone that is programmed to activate a door event flag, such as a button provided inside a door to allow users to exit without using the door reader.
Shunt	A shunt is a procedure that automatically stops a zone input from generating an alarm when it is activated.
Soft time zone	Soft time zones are event-based time zones. They are also referred to as a time zone to follow output.
System bus	The system bus connects DGPs (data gathering panels) and RAS (remote arming stations) to the Alliance control panel.
Tamper	Tampers are situations where a zone input, RAS, DGP, control panel, or associated wiring are tampered with, or accidentally damaged. The tamper feature activates a signal when a tamper alarm occurs.

Table 58. Alliance Builder terms explained (continued)

Term	Definition
Text variable	Numbers used in conjunction with text words. A series of text words and text variables can be used to form phrases such as "Building 6 Area 4 Room 1".
Text word	Text words are words or phrases contained in the database and associated with a number from 1 through 999. Text words in the 1-899 range are predefined in the word library. Text words in the 900-999 range are user-defined and added to the word library.
Time zone	A time zone is a program setting, which identifies specific time periods on specific days. Time zones are allocated to functions to control the activity of the function by time and day and are primarily used to restrict access. See also Soft time zone and Hard time zone.
Upload	Upload is a method to receive information from an Alliance control panel.
User	A user is anyone using the Alliance system. Users are identified to the system with a unique number that is associated with the user's PIN code.
Zone input	A zone input is an electrical signal to the system from a security device such as a PIR detector or door contact. Each device is identified with a zone input number and name.
Zone shunt	A zone shunt procedure prohibits an active zone from generating an alarm during a certain time period.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

V

W

Z

Numerics