tecom

Challenger*Plus* Programming Manual

P/N MAPROG-TS-CHPLUS • REV 2.1 • ISS 30OCT19

Manufacturer
Made in China by United Technologies Safety Systems
No. 80, Changjiang East Road, QETDZ, Qinhuangdao, Hebei,
P. R. China 066004

Imported by UTC Fire & Security Australia Pty Ltd t/a Interlogix
A UTC Climate, Controls & Security company

10 Ferntree Place
Notting Hill, Victoria, 3168, Australia

ACMA compliance

Contact information
For contact information, see www.interlogix.com.au.

Content

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Interlogix (a division of UTC Fire & Security Australia Pty Ltd) be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Interlogix shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Interlogix has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

The customer is responsible for testing and determining the suitability of this product for specific applications. The customer is responsible for testing the product at least once every three months.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Interlogix assumes no responsibility for errors or omissions.

Agency compliance

This product conforms to the standards set by Standards Australia on behalf of the Australian Communications and Media Authority (ACMA). We recommend enclosure covers remain fitted to maintain ACMA compliance.

Regulatory requirements for New Zealand

Some parameters required for compliance with Telecom’s Telepermit requirements are dependent on the equipment (PC) associated with this device. In order to operate within the limits for compliance with Telecom’s Specifications, the associated equipment shall be set to ensure that:

- There shall be no more than 10 call attempts to the same number within any 30 minute period for any single manual call initiation.
- The equipment shall go on-hook for a period of not less than 30 seconds between the end of one attempt and the beginning of the next attempt.
- Automatic calls to different numbers are spaced such that there is no less than 5 seconds between the end of one call attempt and the beginning of another.

- This equipment shall not be set up to make automatic calls to the Telecom ‘111’ Emergency Service.
- The associated equipment shall be set to ensure that calls are answered between 3 and 30 seconds of receipt of ringing.

Preface

This manual applies to the following Challenger*Plus* control panels. The product name “Challenger” will often be used in this manual for Challenger*Plus*.

The *ChallengerPlus Programming Manual* is for system administrators and installers who need to manage the Challenger system via its text-based user interface (in particular the “Install menu”).

Refer also to other Challenger manuals in the suite:

- The *ChallengerPlus Installation and Quick Programming Manual* is for installation technicians to install and commission a Challenger panel.
- The *ChallengerPlus Users Manual* is suitable for most users of the Challenger system to perform everyday tasks.
- The *ChallengerPlus Administrators Manual* is for users and system administrators who need to manage the Challenger system via its text-based user interface (in particular the User menu).

Chapter 1
Introduction

Summary

This chapter provides an overview of the Challenger system.

Content

The Challenger system

Overview

The Challenger integrated alarm and access control panel is widely accepted as a versatile, high-quality product. Challenger's customisable design makes it the benchmark for alarm and access control systems, and Interlogix has been constantly upgrading the capabilities of Challenger and its modular product family to further adapt the product to real-life, ever-changing, applications.

The Challenger panel is the heart and soul of the system, with its modular 'Add as You Go' design. Challenger allows expansion and control of the system with a range of ancillary panels, controllers, readers, and RS-485 LAN devices. Suitable for locations with special needs, Challenger is used in universities, financial institutions, chain stores, supermarkets, and prisons, to name only a few.

The following are some of the features that have made Challenger so popular.

Flexible: Its modular design provides for an amazingly wide range of applications, depending on the number of 'building-blocks' you need to add. Start with just a few access doors and alarm inputs (also called zone inputs), or expand it to control thousands of doors, inputs, and users. Challenger can connect directly to a printer from its own optional interface without needing a dedicated computer or network.

User-friendly: A Challenger system can be programmed and controlled in a variety of ways. A protected area can be both armed and disarmed from a Smart Card Reader, just by swiping the appropriate badge or key fob past the reader (three swipes to arm). The use of a Remote Arming Station (RAS) with a Liquid Crystal Display (LCD) screen or touch screen makes life easy with English text messages to facilitate programming and user input. Interlogix's CTPlus and TecomC4 management software applications provide an even more user-friendly Microsoft Windows®-based programming and control interface.

Scalable: A basic Challenger*Plus* panel (TS-CHPLUS) has sufficient memory to provide access control for 2,000 users. This capacity can be expanded to 65,535 users via a TS1084 Memory Expansion Module. A second RS-485 system LAN can be used to multiply the number of RASs and DGPs to expand the number of readers, inputs, outputs, doors, and so on. Refer to Table 1 on page 3 for details of various models.

Proven reliability: Tens of thousands of Challenger panels are in use today because they have proven to be dependable and stable. In addition, hundreds of trained technicians are skilled at installing and programming Challenger to meet all kinds of needs.

ChallengerPlus capacities

Table 1: ChallengerPlus capacities

Feature	Capacity
Users (expanded)	2,000 (65,535)
Users with names*	2,000
Areas	99
Area Groups	255
Alarm Groups	255
Door Groups	255
Floor Groups	128
Zone inputs	1008
Relays	512
Event flags	255
Time zones	46, with 8 parts
Soft time zones	16
Holidays	24
Holiday types	8
Alarm history events	5,000
Access history events	5,000
Automation zones	100
RS-485 LANs	2
DGPs (total/intelligent)	31/24
RASs	32
Standard doors / lifts	32
Max standard doors	32
Max standard lifts	2
Max floors per standard lift	10
Doors via Controllers	96 (intelligent doors)
Total doors	128 (32 + 96)
Lifts via Controllers	96
Total lifts	98 (2 + 96)
Input shunt timers	32
RAS area-LED mapping	Any areas
RAS relay assignment	Via relay number
Macro logic programs	48
Total disarm areas	Yes
Area search mode	Yes

Financial options	Yes
SD card backup/restore	Yes
Vault programming	Yes

* User names are not stored in the panel when a TS1084 Memory Expansion Module is fitted.

What's new in this release

Challenger*Plus* has the following new features over Challenger10:

- New Input Types. See "Programming twin trip inputs" on page 65 for more information.
- New RAS warning messages. See "Entry and exit console warning" on page 92 for more information.
- New system options for the siren mode (standard 8 Ω siren or 12 Volt DC devices) for both external and internal sirens. See "External siren mode" on page 115 and "Internal siren mode" on page 115 for more information.
- New functionality for lifts. See "Option 44: Standard lifts" on page 201 for more information.
- New functionality for doors. See "Option 45: Standard doors" on page 204 for more information.
- New communication type. See "Connecting via UltraSync" on page 67 for more information.
- New DGP options.

Key features

Experienced Challenger users, installers, and administrators will feel at home with Challenger*Plus* control panels because most of the fundamental concepts are very similar to the Challenger Series and Challenger V8.

The following sections briefly describe the main differences that a programmer will need to know about Challenger*Plus* control panels.

Multiple communication paths

Ten communication paths are available for simultaneous management software connections, reporting via dialler, printing events, and so on. The status of each path can be quickly displayed via RAS to facilitate installation and troubleshooting.

Users

All Challenger users are Intelligent User Memory (IUM) users, and can have PINs up to 10 digits long and up to 48 bits of raw card data.

Expanded capacity

Subject to Challenger model, a second RS-485 LAN may be used to expand the number of Challenger system devices (see Table 1 on page 3).

Zone inputs

The Challenger panel has 16 zone inputs. Every DGP address (31 in total) supports 32 zone inputs for a maximum of 1008 zone inputs.

Notes:

- Some DGP models do not support expansion to 32 zone inputs, so the number of physical inputs at that address is reduced accordingly.
- Zone input numbers in the range 1000 to 1008 will not report CID alarms (Ademco CID format supports 999 zones).

End-of-line (EOL) resistor selection

The Challenger panel can be configured (via system options) for alternative EOL resistor values (default is 10K) for the zone inputs connected directly to the Challenger panel. Alternative EOL resistor values may also be used with zone inputs connected to TS1020 Analogue DGPs.

Areas

The total number of areas has been increased to 99. By default, the first 16 areas are mapped to RAS area LEDs in the same manner as in Challenger V8. If needed, any area number can be mapped to an individual RAS area LED.

Area groups

Area groups are collections of areas that can be more easily managed, for example armed or disarmed simultaneously.

Each area in an area group must be configured to allow certain users (as specified by the user’s alarm group) to have permissions for arming, disarming, alarm reset, and for timing.

Alarm groups

An alarm group can be linked to an area or to an area group:

- If an alarm group is linked to a single area, then the alarm group controls the area’s settings for arming, disarming, alarm reset, and timing (see “Option 5: Alarm groups” on page 96.
- If an alarm group is linked to an area group (one or more areas), then the area group controls each area’s settings for arming, disarming, alarm reset, and timing (see “Option 36: Area groups” on page 190).

User categories

Challenger user categories consist only of a number and a name. All eight user categories can be used for timing via the user category time programmed in Timers.

Holidays

Holidays can be defined for multiple days, and can automatically be repeated annually (on the same dates). A holiday must be assigned a holiday type.

Holiday types

Holiday types consist only of a number and a name. There can be up to eight holiday type records.

Holiday types 1 to 8 are not programmable at the panel (they pre-exist). Each holiday type can optionally have a name in management software, or listed on the Holiday types worksheet (Figure 62 on page 283).

Holiday types provide the ability to grant access for users on some holidays and not others. For example:

- We want cleaning staff to have access during school holidays, but not on public holidays.
- We want maintenance staff to have access during both school and public holidays.
- School holidays can be designated H1 type, and cleaning staff time zone must contain H1 type.
- Public holidays can be designated H2 type, and maintenance staff time zone must contain H1 and H2 types.

Time zones

Time zones can have eight segments, and each segment can be assigned to one or more holiday types.

Relay control groups eliminated

Challenger allows you to directly assign a relay number to the output of a RAS (or Smart Door Controller).

Area search functionality

Area search is a special disarming process to ensure that a facility is safe to enter at the start of the day.

Timed input testing

Timed input testing allows zone inputs to be tested during normal operation within a specified number of days. The Challenger panel can report when an input has been tested and will report an alarm for inputs that haven’t been tested as specified.

Text words replaced by entity names

Challenger*Plus* panels use free text to describe input names, areas, and so on, instead of a limited range of numbers.

Automation zone programming and control

Challenger*Plus* panels provide configuration and control of automation zones (one or more building devices) via technologies such as C-Bus®.

Standard lifts

Challenger*Plus* panels can support up to two standard lifts with ten floors each, without requiring a Four-Lift Controller. See “Option 44: Standard lifts” on page 201 for more information.

Standard doors

Challenger*Plus* panels can support up to thirty-two standard doors, without requiring a Four-Door Controller or Network Access Controller. See “Option 45: Standard doors” on page 204 for more information.

Chapter 2
Overview

Summary

This chapter provides an overview of the Challenger system and instructions for planning the best approach to programming the system.

Content

Product overview

The Challenger panel is the heart and soul of the Challenger alarm and access control system. The Challenger system is essentially a collection of databases that are stored in the panel’s onboard memory and can be programmed by the installer (or administrator, as applicable) using the tools described in the following sections.

LCD RAS

A Challenger system can be programmed and operated via a remote arming station (RAS) that has a keypad with LCD screen.

The RAS’s text-based user interface provides a numbered menu structure for rapid access to the “Install” menus (see Table 3 on page 15). Even if you plan to use management software for most tasks, some initial Challenger system programming must be done using an LCD RAS before it can communicate with management software.

Management software

A Challenger system that is configured and programmed to be accessed via management software (such as CTPlus, Forcefield, or Security Commander) may be programmed and operated via the management software. The management software user interface is graphical and generally follows the RAS programming map. The menu numbers are not used in the graphical interface, and the descriptions of the programming options may vary slightly from the RAS display.

Management software also enables the use of the TS0870P Smart Card Programmer, used to program Smart Cards. Smart Cards can be used for unlocking doors, arming and disarming areas, and for operating ‘credit applications’ such as drinks dispensers, copiers, lighting, and so on.

This manual is based on the programming options as displayed on an LCD RAS. Options listed as YES or NO on the RAS correspond with enabled or disabled, and are typically shown as selected or deselected in the management software user interface.

Planning the system

You should create a system plan prior to installing and programming a Challenger system.

A system plan should include:

- **Site map:** Create a basic drawing that shows the premises with the location of all required system equipment (labelled with name and input number). If the anti-passback function is required for the system, regions and IN/OUT reader addresses should be defined on the site map.

- **Equipment list:** Use the site map to create a list of all equipment needed for the system.
- **Naming convention:** Use the site map to create names for the system's equipment, inputs, relays, areas, and so on. The Challenger panel supports 30 characters for most items.
- **Programming worksheets:** Use worksheets to record programming details and to help understand how the various programming options relate to each other. Worksheets (typically completed by the installer) may be found in Appendix B "Programming worksheets" on page 249.

In planning the system make sure you define what outputs (siren, strobe, relays) will be required. This will determine the event flags that will need to be programmed in the input, area, arming station, summary event flags, and shunt timer databases.

Refer to the *ChallengerPlus Installation and Quick Programming Manual* for installation and setup information.

Enclosure Access Restrictions

According to the requirements of AS/NZS 60950-1, the interior of the enclosure presents hazards to general users and thus physical access restrictions must be instituted ensure safety. To comply with the requirements related to safety:

- Access to the interior of the Enclosure must be limited to suitably trained and qualified installation and maintenance technicians.
- Access to the interior of the enclosure should require the use of a tool.

These restrictions can be met by suitably securing the enclosure door as follows:

- Fit a lock to the enclosure. Ensure that it is always locked when not under the immediate control of suitably qualified technicians.
- Seal the enclosure door using standard head (non-knurled) screws, firmly tightened.
- When using finger operable screws (knurled head, etc) to seal the enclosure door, tighten to 2Nm (typically >1/4 turn beyond the finger tight point).

Battery Specifications

The ChallengerPlus should be connected to sealed lead acid (SLA) batteries (not supplied) compliant with AS/NZS 2201.1:2007. The batteries must have a nominal terminal voltage of 12V and must have an initial charging current limit >1.5A.

The installer is responsible for identifying and specifying batteries with an operating temperature range commensurate with the specific TS1066 installation environment; a minimum range of 0°C to +40°C is recommended.

A fuse is required in the positive lead of each battery. Each fuse must be a 3AG/3AB (6x32 mm) 8A, 250 VAC, slow blow (time lag) fuse, compliant with UL 248.14. Suitable parts include Littelfuse 0313008.HXP, Bel Fuse 3SB 8-R, and Schurter 8020.5020.

The installer is responsible for ensuring that the specified batteries in conjunction with the configured system load and TS1066 charger settings provide the required system backup and recharge times.

The installer (or user) is responsible for scheduling on-going battery system checks as required by the applicable standards and codes to ensure user safety, battery integrity and system performance; a 3 monthly interval is suggested.

Chapter 3
Programming basics

Summary

This chapter provides instructions for getting started with programming the Challenger system.

Content

User menu structure

There are 24 top-level User menus in the Challenger system (see Table 2 below).

Most of the programming described in this manual is in sub-menus accessed via option 19. Install Menu (see Table 3 on page 15). However, you may need User menu options 14, 15, 20, and 21 when programming the system. Refer to the *ChallengerPlus Administrators Manual* for information about these top-level menus.

Table 2: User menu (top level)

User menu option	Description
1. Panel Status	Lists inputs in alarm, tamper, isolated, unsealed, and system alarms.
2. Input Unsealed	Lists unsealed inputs, for example, an open door contact or an input in tamper condition.
3. Input In Alarm	Lists inputs in alarm.
4. Input Isolated	Lists inputs that are isolated.
5. History	Lists events of system history, including alarms, menu access, etc.
6. Test Report	Displays the results of the access test or secure test.
7. Service Menu	Request a service call or connect/disconnect to management software.
8. Film Counters	Display the frame number position on security camera films.
9. Input Text	Display the description of the inputs.
10. Isolate	Isolate inputs.
11. Deisolate	Deisolate inputs.
12. Test Input	Test an individual input device.
13. Start Auto Access Test	Start the access test.
14. Program Users	Create, modify, or delete user records.
15. Time and Date	Program the panel's time and date.
16. Isolate/Deisolate RAS/DGP	Isolate or deisolate RASs or DGPs.
17. Enable/Disable Service Tech	Enable and disable the service technician's PIN.
18. Reset Cameras	Reset the film frame count on security cameras.
19. Install Menu	See Table 3 on page 15.
20. Door and Floor Groups	Program door and floor groups.
21. Holidays	Record the dates of holidays.
22. Open Door	Open a door.
23. Unlock, Lock, Disable and Enable	Unlock, lock, disable, or enable a door.

User menu option	Description
24. Automation Control	Turn automation zones (such as lights) on or off.
25. Change PIN	Change default PIN.

Install menu structure

Table 3 below lists the Install menu options, accessed via User menu option 19. The Install menu items are described in detail in Chapter 5 “Command reference” on page 68.

The Challenger menus contain numbered options. The option numbers help to navigate the text-based interface on an LCD RAS and not provided as a guide to programming sequence or other workflow. Refer to “Setting up a basic alarm system” on page 24 for the recommended programming sequence.

Table 3: Install menu

Install menu option	Description
1. Input Database	Define every input (physical input on the control panel, DGP, or plug-in expander, and inputs that are activated by macros).
2. Area Database	Define up to 99 areas. Areas determine how the system is partitioned, and therefore provides the ability to limit users to performing functions only in the areas relevant to their role.
3. RAS Database	Define the system’s remote arming stations (RASs). RASs provide alarm system control, such as area arming or disarming; and provide access control, such as unlocking a door for a user.
4. DGP Database	Define any data gathering panels (DGPs) used to send information to the control panel and to provide added access control functionality (when using Intelligent Access Controllers).
5. Alarm Groups	Define alarm groups to enable users, inputs, and arming stations to control the system’s alarm control functionality.
6. Timers	Define the system’s timers if the default values are not suitable.
7. System Options	Define the system options if the default values are not suitable.
8. Auto Reset	Program the Challenger to automatically reset alarms.
9. Communications	Program the hardware devices and communications paths that the panel will use.
10. Reserved	Not used in this version.
11. Version	Display the system’s device types and firmware version numbers.
12. Lamp Test	Toggle the on/off state of all RAS LEDs in the system so that they may be checked.

Install menu option	Description
13. Time Zones	Define time slots ('hard' time zones) in which certain events can take place.
14. Defaults	Reset the panel to default settings.
15. User Category	User categories provide timing for areas that are configured for timed disarming or for delayed arming (via vault programming).
16. Map Relays	Link relays (outputs) to event flags and/or time zones.
17. Arm/Disarm via Tz	Define arm/disarm timer programs. Areas being armed or disarmed automatically (by time zone) do not require any user action.
18. Vaults	Define areas that, when armed, will automatically arm other areas after a specified time.
19. Area Linking	Define a common area that is armed when the last shared area is armed.
20. Reserved	Not used in this version.
21. Input Shunts	Define shunt timers to inhibit inputs from generating alarms during a specified interval.
22. Soft time zones	Define soft time zones. Time zones 26 to 41 can be programmed to be valid when a relay is active and invalid at other times.
23. Poll Errors	Display the number of errors detected in communications between the control panel and the devices connected to the control panel.
24. Send Programming	Send access control data for Intelligent Access Controllers (4-door or 4-lift DGPs) that may not have been sent automatically.
25. Display Last Card	Display the RAS number and card data of the last card read by a reader connected directly to the control panel (for doors 1 to 16 on LAN 1 and doors 65 to 80 on LAN 2).
26. Diagnostics	Skip this option. It is reserved for factory use.
27. Reserved	Not used in this version.
28. Remote Controllers	Access additional programming menus for remote devices such as a RAS, an Intelligent Access Controller DGP, or a TS0862 Smart Door Controller (which is addressed and polled as a RAS).
29. Panel Volts & Currents	Display the values of the panel's voltage and current consumption.
30. Reserved	Not used in this version.
31. Battery Testing	Program automatic battery testing or perform manual battery testing.
32. Custom Message	Create a custom message (or use the panel's time and date) for the top line of the RAS's initial LCD screen.
33. Program Next Service	Program the date of the next service call, and a custom message on the LCD to call the installer.

Install menu option	Description
34. Program Summary Event Flags	Program event flags to be triggered on system-wide events such as mains failures or DGPs going offline.
35. Program Macro Logic	Program macro logic equations for activating inputs or event flags based on the conditions of one to four macro inputs (event flags or relays).
36. Area Groups	Area groups include one or more areas that can be more easily managed, for example armed or disarmed simultaneously. Each area in an area group must be configured to allow certain users (as specified by the user's alarm group) to have permissions for arming, disarming, alarm reset, and for timing. Area group 1 contains areas 1 to 99 by default (1 to 16 for TS1016LE).
37. SD Card Backup/Restore	Challenger*Plus* panels have an onboard SD card port to back up a panel's programming, or to restore a panel's programming from a previously-saved backup file.
38. Reset Input Test Days	After programming timed input testing the installer may need to reset the input timer before handing the system over to the customer.
39. Automation	Program automation zones such as C-Bus devices to be controlled via the Challenger panel.
40. Door Setup	Program a door's name, event flag and event flag trigger duration (typically for use as an automation zone trigger).
41. Event Flags	Assign names to the Challenger panel's event flags.
42. Challenger Name	Assign a name to the Challenger panel.
43. Automation Status	Check and control automation zones via from any LCD RAS.
44. Standard lifts	Program up to two standard lifts of up to ten floors each.
45. Standard doors	Program up to sixteen standard doors.

Disarming the system

The system must be completely disarmed (all areas) before you can access the Install menu. Use the following steps to disarm the system.

1. The default message displays on the top line of the RAS. Depending on the programming of "Option 32: Custom message" on page 182, this line may display "There Are No Alarms In This Area", the time and date, or a custom message.

```
There Are No Alarms In This Area
Code:
```

2. Press 4346 (the default Installer code), press [OFF] [0] (to select all areas), and then press [ENTER].

Accessing the Install menu

The Challenger menu system, as displayed on an LCD RAS, has a first-level User menu and a second-level Install menu (the Install menu is option 19 of the User menu). Access to the Install menu is typically limited to installers or administrators.

Use the following steps to access the Challenger User menu when the Code prompt is displayed on the bottom line of the RAS.

1. Press [MENU*].

```
To Access Menu Enter Code
Code:
```

2. Enter 4346 (default Installer code), and then press [ENTER].

```
"0"−Exit  "ENTER"−Down  "*"−Up
0−Exit, Menu:
```

3. You can now select the programming option you need from the User menu (see Table 2 on page 14). To access the Install menu, enter 19 (Install menu option number), and then press [ENTER].

```
Install Menu
0−Exit, Menu:
```

You can now select the programming option you need from the Install menu (see Table 3 on page 15).

Reset to default

Sometimes it is necessary to bring the control panel back to factory defaults (for example, if programming a system that has been without power for more than two weeks). Refer to “Option 14: Defaults” on page 163 for instructions.

Alternatively, you may need to default the panel without using the Install menu. Refer to “Clearing the memory via the Challenger panel PCB” in the *ChallengerPlus Installation and Quick Programming Manual*.

Programming via RAS

Common navigation techniques

The following keys are used to move between menus or between menu options in the Install menu:

- Press [ENTER] to scroll forward one menu option.
- Press [MENU*] to scroll backward one menu option.

- Enter the menu number and press [ENTER] to jump directly to a menu.
- Enter [0] and press [ENTER] or press [CLEAR] to exit the menu.

Model-specific navigation techniques

Certain RASs have additional navigation options, as described in the following sections.

TS1001

The TS1001 Touch Screen RAS has a graphical touch screen to simplify navigation, reduce the number of button presses required, and facilitate text entry. It also has a Classic mode that mimics a conventional LCD keypad. Refer to the *TS1001 Touch Screen Arming Station User Manual* for details.

CA111x-series

Use the up and down arrow keys to move backwards and forwards through a record’s options. For example, if you are programming an input you can back up to an option if you go past it. Also, you can move backwards instantly from the first option to the last option.

Use the left and right arrow keys to move backwards and forwards between records (such as inputs) for the same field. For example, you can enter a name for input 1, press [ENTER] to save, and then press the right arrow key to enter a name for input 2, and so on. When going backwards between records you can press the left arrow button to move immediately from the first record to the last record.

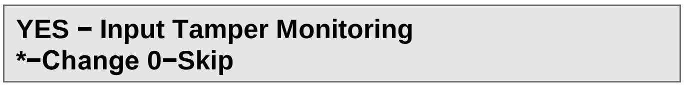
TS0801 and TS0802

Use the up and down arrow keys (ON and OFF keys) to move backwards and forwards through a record’s options. For example, if you are programming an input you can back up to an option if you go past it. Also, you can move backwards instantly from the first option to the last option.

The LCD screen

The LCD screen (or touch screen) on the RAS has at least two lines of characters. Each line contains a different type of information.

Figure 1: Sample LCD message to toggle a value



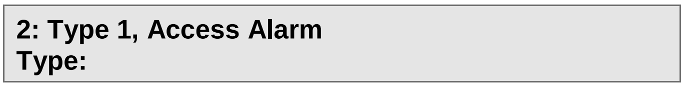
YES − Input Tamper Monitoring
***−Change 0−Skip**

For example, the top line in Figure 1 above contains system information, and the bottom line contains the instructions and characters you can enter on the keypad. For this example, you could:

- Press * to toggle the YES/NO value, and then press [ENTER] when correct.

- Press [0] to skip this option.

Figure 2: Sample LCD message to enter a value



2: Type 1, Access Alarm
Type:

For example:

- The top line in Figure 2 above identifies the item being programmed (in this example, input 2) followed by its currently programmed value.
- The bottom line describes what’s being programmed (in this example, input type) followed by the characters (if any) that you entered on the keypad.

Programming the options

In this document, “enter” is used in the following ways:

- Press the key (or sequence of keys) on the RAS keypad that corresponds with the required value. For example, press the [0] key to ‘enter’ the value 0.
- Press the [ENTER] key on the RAS keypad to accept the value that you entered (or to accept the value displayed on the LCD).

To program a YES/NO option (Figure 1 on page 19), press [ENTER] to accept the displayed value or press [MENU*] to toggle between YES and NO. Press [0] to skip options.

To program a value such as a number or amount (Figure 2 above) enter the value, and then press [ENTER]. The information will be saved and the display will show the next option.

Note: If a value is already programmed and needs to be changed, enter the new value (or toggle, if applicable), and then press [ENTER] to change the value.

Selecting areas by searching

Areas are identified by a number and (optionally) a name programmed by the installer.

When arming or disarming the system, you may want to select a specific area instead of selecting all areas. Some RAS models (such as the CA111x series) allow you to quickly find areas by name.

For example to use a CA1116 RAS to arm an area named “East wing foyer”:

1. Press nnnn (where nnnn is your code), and then press [ENTER] or [ON]. Any disarmed areas that are assigned to your alarm group are listed.

2. Press the multi-function key to begin (on the CA1116 RAS the multi-function key is the left-hand “—” key).

```
Area Search is ,(*)−End
```

3. Use the RAS keypad to enter a search character or string. When each character is displayed, press [ENTER] to move to the next position. When finished, press [*] to list all areas that contain the string.

   For example, search for “EAST” to find all with area names beginning with that text (including “East wing foyer”). Search is not case-sensitive.
4. When the list of areas displays, you can press the area number and then press [ENTER] to arm only that area. Alternatively, press [0] [ENTER] to arm all of the found areas.
5. When finished arming areas, press [ENTER] to exit the display.

Refer to Table 5 on page 62 or “Entering text via RAS” in the *ChallengerPlus Administrators Manual* for details.

Programming sequence

Program the system in the order listed in “Setting up a basic alarm system” on page 24. All remaining Install menu options may be programmed in any order to suit individual installations.

Default installer PIN

Changing the default installer PIN

The default panel programming includes PIN 4346 for user 50. The default PIN must be changed to keep unauthorised persons from modifying your programming or using the system without authorisation.

Restoring the default installer PIN

If the installer PIN for user 50 has been changed and lost, you may need to reset the PIN to default (4346). This is easily accomplished via management software. However, if necessary, it can be done from the Challenger panel PCB.

To restore the default installer PIN:

1. Access the Challenger panel PCB.
2. Fit test link 1 momentarily, and then remove the link.

Refer to the *ChallengerPlus Administrators Manual* for details.

Chapter 4
Common tasks

Summary

This chapter provides an overview of the programming needed to perform various tasks within the Challenger system. Understanding these tasks helps you to understand how various panel programming concepts are related to each other.

Content

Setting up a basic alarm system

Overview

This section provides an overview of how to use an LCD RAS to set up a basic alarm system that uses PINs for access control.

Use the following steps to set up a basic alarm system:

1. Plan the system and fill out the programming sheets. See “Planning the system” on page 10.
2. Disarm the system. See “Disarming the system” on page 17.
3. Access the Install menu. See “Accessing the Install menu” on page 18.
4. Default the system. See “Option 14: Defaults” on page 163.
5. Disarm the system and access the Install menu again, as described above.
6. Program the date and time in User menu option 15, Time and Date.
7. Optional: Change the default installer PIN. See “Default installer PIN” on page 21.
8. Program the required system options if the default values are not suitable (see “System option defaults” on page 28). The only options you need to consider for a basic alarm system are as follows:
    - “Test mode” on page 110.
    - “No. of Relay controllers” on page 111.
    - “Input tamper monitoring” on page 115.
    - “Display one input at a time” on page 116.
    - “Name file” on page 116.
    - “System alarms set siren and strobe” on page 116.
    - “System alarms” on page 117.
    - “Disable code from displaying” on page 118.
    - “Disable flashing area LEDs” on page 118.
    - “Display alarms instantly on LCD” on page 118.
    - “Sirens only after report fail” on page 118.
9. Program time zones using “Option 13: Time zones” on page 161.
10. Program holidays in User menu option 21. Holidays.
11. Program areas using “Option 2: Area database” on page 77.
12. Program alarm groups using “Option 5: Alarm groups” on page 96.
13. If your system requires more than 16 inputs, or requires advanced access control functionality, then you will need to program DGPs (data gathering

panels) into the system. Program DGPs using “Option 4: DGP database” on page 93.

14. Program inputs using “Option 1: Input database” on page 70.
15. If your system requires more than one arming station, then you will need to program RASs. The only options you need to consider for a basic alarm system are as follows:
    - “RAS model

Select the RAS model attached to the ChallengerPlus panel. This will allow certain options in the panel to be configured to ensure optimal communications.

```
1:RAS Model is:
Model No:
```

The model may be selected from a pre-defined list, as detailed in Table 8.

Table 8: RAS models summary

Model No	RAS model	LCD	Keypad	Card Reader	Mag Swipe	LEDs
1	TS0003		Yes			4
2	TS0004	Yes	Yes			16
3	TS0006		Yes			4
4	TS0007		Yes		Yes	4
5	TS0008		Yes		Yes	4
6	TS0801	Yes	Yes			8
7	TS0804	Yes	Yes			16
8	TS0862			Yes		2
9	CA1110	Yes	Yes			16
10	CA1111	Yes	Yes			16
11	CA1115	Yes	Yes	Yes		16
12	CA1116	Yes	Yes	Yes		16
13	TS0870			Yes		2
14	TS0870H			Yes		2
15	TS0870D			Yes		2
16	TS1001	Yes	Yes			8
	TS1162		Yes			3

Area alarm group” on page 86.

- “Menu alarm group” on page 87.
- “LCD arming station” on page 89.
- “Toggle keyboard control” on page 89.

16. Program the system’s timers if the default values are not suitable (see “Timer defaults” on page 28):
    - “User category time” on page 104.
    - “Access test time” on page 105.
    - “Secure test time” on page 105.
    - “Warning time” on page 105.
    - “Delay holdup time” on page 105.
    - “Suspicion time” on page 106.
    - “Service time” on page 106.
    - “Local alarm reminder time” on page 106.
    - “Individual input test time” on page 106.
    - “Door(s) unlock time” on page 106.
    - “Tester event flag time” on page 107.

- “Siren time set to” on page 107.
- “Mains fail time” on page 107.

17. Program the communication options to enable the Challenger system to report alarms to the remote monitoring station. See “Option 9: Communications” on page 122.
18. Program the behaviour of relays using “Option 16: Map relays” on page 165.
19. Reset all poll error counters when the system is error-free. Otherwise, errors that occurred during installation and programming could distort future error counts. See “Option 23: Poll errors” on page 176.
20. Program (at least) the first user. See “Programming users” on page 29.

Default programming values

The Challenger panel is supplied with a set of factory defaults in the programming to make initial set-up easier. The default settings are as follows.

Input defaults

- Input type is set to type 2 Secure Alarm (inputs 1 to 16 only)
- Report ID type is set to 25-140, General Alarm
- Assigned to area 1
- Siren event flag is selected
- Event flag 2 Secure Alarm is selected, and is mapped to relay 2 Strobe Output

Area defaults

- Areas 1 to 16 have names
- Exit time is set to 60 seconds
- Entry time is set to 30 seconds
- Siren event flag is set to 1

Area group default

- Area Group 1 (used by master installer, master user, and master RAS alarm groups) contains areas 1 to 99

Arming station defaults

- RAS 1 is polled
- RAS 1 is LCD arming station
- RAS 1 has LEDs 1 to 16 mapped to areas 1 to 16
- RAS 1 has Alarm Group 2 (Master RAS)

System option defaults

- Film Low is set to 800
- Film Out is set to 1100
- Relay Controllers is set to 0
- Input tamper monitoring is selected
- Display one input at a time is selected
- User name file is selected
- EOL Resistor Code is set to 0 (10K Ohm)
- Time zone is set to 0 (not used)
- Area search time zone is set to 0 (not used)
- External siren mode is set to 0 (standard 8 Ω siren speaker)
- Internal siren mode is set to 0 (standard 8 Ω siren speaker)

Timer defaults

- Each user category time is set to 0 minutes
- Access test time is set to 15 minutes
- Secure test time is set to 15 minutes
- Warning time is set to 5 minutes
- Delay holdup time is set to 60 seconds
- Suspicion time is set to 15 seconds
- Service time is set to 30 minutes
- Local alarm reminder time is set to 0 minutes
- Individual testmode time is set to 5 minutes
- Door/s unlock time is set to 5 seconds
- Tester event flag time is set to 15 seconds
- Siren time is set to 8 minutes
- Mains fail time is set to 0 minutes
- Card to code time is set to 8 seconds
- Minimum area search time is set to 0 minutes
- Maximum area search time is set to 0 minutes
- Maximum twin trip time is set to 60 seconds

Relay mapping defaults

- Relay 2 (panel strobe output) is mapped to event flag 2

- Relay 16 (panel siren driver) is mapped to event flag 1. The sixteenth relay assigned to each DGP (DGP siren drivers relay 32, 48, 64 and so on) is also mapped to event flag 1.

User defaults

- User 50, the master code is allocated:
  - Name TECOM Master
  - PIN 4346
  - Alarm Group 3 (containing Area Group 1)
  - Door Group 1
  - Floor Group 1

Programming users

The installer must initially program a user into the system who has the necessary authority to program additional users into their system.

It is important that the client is provided with details of the users' alarm groups to facilitate this. Use "Alarm group worksheet" on page 257 to list the alarm groups that the client will use when adding or changing users in their system.

Use the following steps to create a user or modify an existing user:

1. From the Challenger User menu (see "User menu structure" on page 14) select option 14. Program Users.
2. Select option 3. Create.
3. Select a user number to program.

   Note: User number 50 is the Master Installer Code. The PIN for user 50 should be changed from the factory default of 4346, but no other parameter should be altered.

4. Assign an alarm group to the user to specify the areas and functions allowed. It is not necessary to assign a door group or a floor group for a basic alarm system using PINs for control. See "Option 5: Alarm groups" on page 96.
5. Program the user's name (applies only to user numbers 1 to 2,000).
6. Program the user's PIN.
7. If you want the user to be activated from a particular date, then program a start date and time.
8. If you want the user to be deactivated at a later date, then program an end date and time.

Note: When programming a new user record in User menu option 14. Program Users, a list of designated “user alarm groups” are displayed on the RAS for assigning to the new user. The list of designated “user alarm groups” depends on the alarm group (and alternate alarm group, if applicable) of the person doing the programming. You cannot assign an alarm group to a new user that has more permissions than you have.

Programming relays

This section provides an overview of how to program relays and outputs in the Challenger system.

Overview

Relays may be used for a variety of applications, including:

- Sirens (timed or untimed) and strobes.
- Door locks.
- Warning beepers and lamps.
- Activating cameras.
- Mimic LEDs or lamps for inputs, area and system status, system fault indication.
- Automatic testing of input devices (for example, seismic detectors).
- Interface to building management systems (lighting, heating, air conditioning, and so on).
- Activate backup communicators.
- Link functions together within the system (physical relay not required).

If open collector outputs are required for any of these applications (for example, mimic LED panels), a 16-way open collector card is available. For programming purposes, each open collector output is treated as a relay.

Programming steps

1. Note the type and quantity of relay cards used and which unit (panel or DGP), the relay cards are connected to.
2. Configure the panel or DGP as required to use the relay cards.
   - To configure the panel, refer to “No. of Relay controllers” on page 111.
   - To configure an Intelligent Access Controller DGP, refer to the Intelligent Access Controller Programming Manual for details of programming the relay controllers option.

- For DGPs TS0820 or TS0824, set the DIP switch segment 6 to ON if a TS0841 or TS0842 relay controller is connected to J8 or J9, or OFF if a TS0840 4-Way Relay Card is connected.

3. Determine the number of the relays you wish to program. The relay numbers allocated for the panel and each DGP address are listed in Table 25 on page 225.
4. Use the 16 predefined event flags (Table 30 on page 243) or program user-defined event flags to activate your relays.
5. Determine or program any ‘hard’ time zones that may be required to control your relays (a relay can be programmed to be held active or inactive during a time zone). Time zones are programmed in “Option 13: Time zones” on page 161.
6. Program the details for each of the relays in your system, in “Option 16: Map relays” on page 165.

Example

The “Mulgrave” site has two 8-way relay cards (TS0841) connected to the Challenger panel number 1.

Normal business hours are 8:00 am to 5:30 pm Monday to Friday, and 8:00 am to 12:30 pm Saturday.

Relay 15 is required to interface to a lighting system to automatically turn the lighting on during normal business hours or if the building security is turned off (Area 1 in access).

The relevant programming details in “Option 7: System options” on page 108 is:

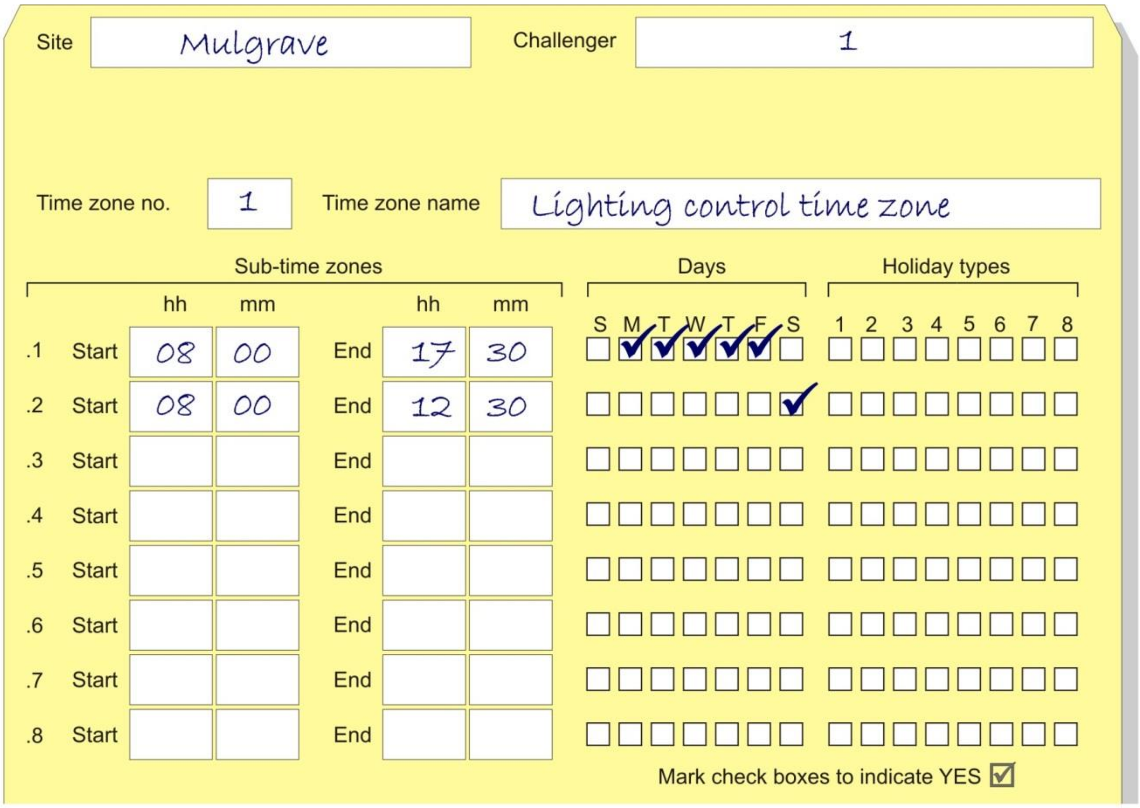
- Number of relay controllers is 2.

The relevant programming details in “Option 2: Area database” on page 77 are:

- Area number is 1.
- Area Accessed Event Flag number is 17 (this is the first user-defined event flag).

The relevant time zone programming details are shown the worksheet example in Figure 3 on page 32.

Figure 3: Time zones worksheet example



Site Mulgrave

Challenger 1

Time zone no. 1

Time zone name Lighting control time zone

		Sub-time zones					Days							Holiday types							
		hh	mm		hh	mm	S	M	T	W	T	F	S	1	2	3	4	5	6	7	8
.1	Start	08	00	End	17	30	□	☑	☑	☑	☑	☑	□	□	□	□	□	□	□	□	□
.2	Start	08	00	End	12	30	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□
.3	Start			End			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
.4	Start			End			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
.5	Start			End			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
.6	Start			End			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
.7	Start			End			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
.8	Start			End			□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Mark check boxes to indicate YES ☑

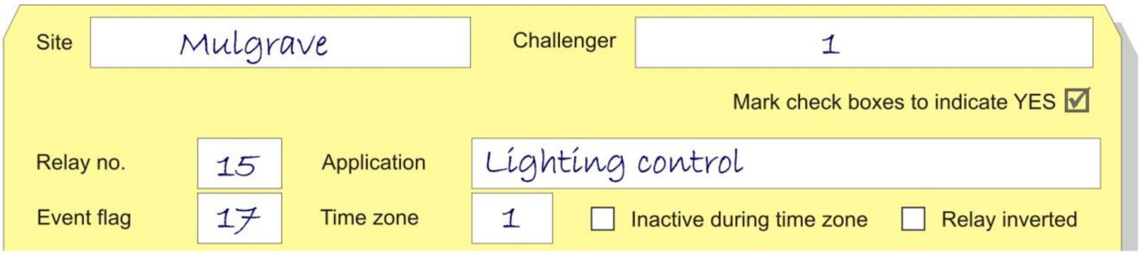
The relevant programming details in “Option 16: Map relays” on page 165 are:

- Relay number is 15.
- Event Flag number is 17.
- Time zone number is 1.
- Active during time zone.
- Non-inverted.

In addition, you might want to record the relay’s application such as “lighting control” on the “Relay mapping worksheet” on page 269. This detail is for future reference only and is not programmed into the system.

Figure 4 below is an example of a worksheet detail for this example of relay mapping.

Figure 4: Relay mapping worksheet example



Site Mulgrave

Challenger 1

Mark check boxes to indicate YES ☑

Relay no. 15

Application Lighting control

Event flag 17

Time zone 1

□ Inactive during time zone

□ Relay inverted

Connecting to a printer

The Challenger panel’s printer output may be used for:

- Printing events on a printer (such as Epson-compatible dot matrix or HP IIP-compatible laser printer) connected by a serial cable to the Challenger panel’s J15 (STU) terminals. See “Printer output via RS-232” below.
- Sending events to a computer via IP connection to the Challenger panel’s Ethernet port at J19. See “Printer output via IP” on page 34.

Printer output via RS-232

Use the following steps to print from a printer (such as Epson-compatible dot matrix or HP IIP-compatible laser printer) connected to the Challenger panel’s onboard RS-232 STU port (J15).

You will need to obtain or make a cable to connect the J15 terminals to your printer.

Refer to your printer documentation to determine the settings you will need to program in the Challenger panel.

For Epson printers the range of parameters includes:

- Baud: 9600
- Data bits: 8 (not configurable in Challenger)
- Parity: None, Odd, or Even
- Stop bits: 1

For HP IIP printers the range of parameters includes:

- Baud: 9600 or 19200
- Data bits: 8 (not configurable in Challenger)
- Parity: None
- Stop bits: 1

To connect a printer via RS-232:

1. Connect the printer to the Challenger panel’s onboard RS-232 STU port (J15).
2. Program a time zone if you require the printer to be enabled or disabled during specific time periods (see “Option 13: Time zones” on page 161). Time zone 0 is valid 24 hours every day. It may be used wherever a 24-hour time zone is required.
3. From Install menu option 9 Communications, select option 1 Setup, to access the Setup menu.
4. From the Setup menu, select option 1 Onboard to configure the onboard serial port.

5. Program the baud, parity, and stop bits to suit your printer.
6. Select option 2 Paths, and then create a new (unused) communications path record for the printer (for example, path 4 because paths 1, 2, and 3 are set up for reporting by default).
7. Press Enter to display the first item in the path menu.
8. Select option 1 Main, and then program the format “Printer”, program the sub-format to suit your printer, and then select Enable.

Printer output via IP

You can send the Challenger panel’s printer data via IP to a computer. The data can be used in third-party applications, such as Nurse Call systems.

Note: Events such as alarms are not acknowledged. The Challenger panel cannot resend events that are not received.

To send printer output via IP:

1. Connect the Challenger panel’s onboard Ethernet port to the network.
2. Program a time zone if you require the printer to be enabled or disabled during specific time periods (see “Option 13: Time zones” on page 161). Time zone 0 is valid 24 hours every day. It may be used wherever a 24-hour time zone is required.
3. From Install menu option 9 Communications, select option 1 Setup, to access the Setup menu.
4. From the Setup menu, select option 1 Onboard to configure the onboard Ethernet port.
5. Enable the Ethernet option and program other IP-related options as required.
6. Select option 2 Paths, and then create a new (unused) communications path record for the printer (for example, path 4 because paths 1, 2, and 3 are set up for reporting by default).
7. Press Enter to display the first item in the path menu.
8. Select option 1 Main, and then program the format “Printer”, program the sub-format to suit your requirements (typically None), and then select Enable.
9. Select option 2 Path Connection Control, and then change the Always Connect option to Yes.
10. Select option 6 Path IP Address, and then program the Send to IP address (the IP address of the computer to which you want to send the printer data).
11. Program the Send IP Port number (for example, 3001) that will be used for sending data to other devices.
12. Select UDP/IP for the IP mode.

Connecting to software

Challenger panels may connect to computers running management software such as CTPlus or TecomC4.

Ten communication paths are available for simultaneous management software connections, reporting via onboard dialler, printing events, and so on.

Connection options include:

- Serial (RS-232) connection via the Challenger panel’s STU terminals
- Modem connection via the Challenger panel’s dialler (if applicable).
- Ethernet connection via the Challenger panel’s Ethernet port
- USB connection via the Challenger panel’s USB port
- Cellular (4G) connection via an optional plug-on module
- UltraSync connection via Ethernet or 4G.

Refer to “Enabling communications” in *ChallengerPlus Installation and Quick Programming Manual* for details.

Programming arming stations

This section provides an overview of programming requirements for keypads and card readers.

Introduction

Remote arming stations (RASs) have LEDs to indicate area and system status. The number of area LEDs determines the RAS’s suitability for controlling a single area or multiple areas.

The areas that the RAS can control are determined by the area alarm group assigned to the RAS. RASs with 2, 3, or 4 LEDs are suitable for single-area alarm groups (for example, alarm groups 14 to 29). RASs with 8 or 16 LEDs are suitable for multi-area alarm groups because each LED can correspond to an area. Any area LED can be mapped to any of Challenger’s 99 areas.

Refer to Table 8 on page 87 for a list of common RASs and related features.

Keypad arming stations

Keypad RASs are used to enter data into the Challenger system. RASs that have only a keypad can be used only for entering a PIN and performing basic alarm control and access control functions. RASs that have a keypad plus LCD, or a touch screen, are used to program the Challenger system.

Use the following steps to program a keypad RAS.

1. Determine how the RAS is to be used in the system and fill out the appropriate programming sheets.
2. Optionally, specify the alarm code prefix value (see “Number of prefix ” on page 112). The alarm prefix allows a PIN of 5 digits or more to be used for the alarm control functions and a shorter code (minimum 4 digits) to be used just for door access.
3. Program any time zones that may be required in order to limit the alarm or access control functions of the RAS to specific time periods. See “Option 13: Time zones” on page 161.
4. Determine whether an existing alarm group is suitable for the RAS. Program a new alarm group if necessary in “Option 5: Alarm groups” on page 96.
   - If the RAS does not have an LCD, the alarm group’s User menu options do not apply.
   - If alarm control is needed, the alarm group must have Alarm System Control enabled, plus any other options, as required.
5. Program the RAS’s specific details in “Option 3: RAS database” on page 83 including the following:
   - Area alarm group. The area alarm group defines the areas, alarm control and User menu options available at this RAS.
   - Menu alarm group. The menu alarm group specifies User menu options available if requirements are different from those specified in the area alarm group.
   - Door event flag. If the RAS is to activate a relay to unlock a door, then a door event flag number must be entered. Enter any event flag number that is not used elsewhere in the system. If you know the number of the relay that is to be used to unlock the door, you may choose to make the event flag number the same.
   - Relay number. If the open collector output on the RAS is to be used to activate a warning buzzer, relay, and so on, then a relay number must be assigned to the RAS.
   - Other options appropriate to the RAS and its application. See “RAS programming options” on page 89.
6. Program door groups to specify which doors (RASs) a user may access. Door groups are programmed in User menu option 20.
7. If the RAS is activating a relay to unlock a door:
   - Program the door’s unlock time in “Option 6: Timers” on page 104. The default is 5 seconds.
   - Determine the relay number to use. See “Relay and output numbering” on page 226 for details.

- Program the details in “Option 16: Map relays” on page 165.

8. If an input is required to be shunted (disabled) for a period of time when the door access function is performed at the RAS, program shunt options in “Option 21: Input shunts” on page 171.
9. Ensure that any users who are to perform any access control functions with the RAS have an appropriate door group assigned to them. See “Programming users” on page 29.

Card reader arming stations

RASs that have card readers or magnetic swipe readers may also have keypads and LCDs. Refer to “Keypad arming stations” on page 35 for details of programming RASs with a combination of features.

This section describes how to program RAS that have a card reader or magnetic swipe reader (and two LEDs). Such RASs will be called ‘readers’ in this section. Readers are programmed as RASs, and can be used to perform alarm control functions and/or to access a door.

Use the following steps to program a reader.

1. Determine how the reader is to be used in the system and fill out the appropriate programming sheets.
2. Program any time zones that may be required in order to limit the alarm or access control functions of the reader to specific time periods. See “Option 13: Time zones” on page 161.
3. Determine whether an existing alarm group is suitable for the reader. Program a new alarm group if necessary in “Option 5: Alarm groups” on page 96.
    - If the card reader does not have an LCD, it can't display menus. However, we recommend that the alarm group that is used as the RAS's area alarm group is also used as the menu alarm group.
    - If alarm control is needed, the alarm group must have Alarm System Control enabled, plus any other options, as required.
4. Program the reader’s specific details in “Option 3: RAS database” on page 83, including the following:
    - Area alarm group. The area alarm group defines the area, alarm control and User menu options available at this reader.
    - Menu alarm group. If the card reader does not have an LCD, it can't display menus. However, we recommend that the alarm group that is used as the RAS's area alarm group is also used as the menu alarm group.
    - Door event flag. If the reader is to activate a relay to unlock a door, then a door event flag number must be entered. Enter any event flag number that is not used elsewhere in the system. If you know the number of the relay

that is to be used to unlock the door, you may choose to make the event flag number the same.

- Relay number. If the open collector output on the reader is to be used to activate a warning buzzer, relay, and so on, then a relay number must be assigned to the reader.
- Other options appropriate to the reader and its application. See “RAS programming options” on page 89 and “Using card readers for alarm control” below.

5. Program door groups to specify which doors (readers) a user may access. Door groups are programmed in User menu option 20.
6. If the reader is activating a relay to unlock a door:
   - Program the door’s unlock time in “Option 6: Timers” on page 104. The default is 5 seconds.
   - Determine the relay number to use. See Table 25 on page 225 for details.
   - Program the details in “Option 16: Map relays” on page 165.
7. If the open collector output on the magnetic card reader or the “LO” open collector output on the Wiegand interface are to be used to activate a relay for the lock, refer to (“Relay and output numbering” on page 226) for details.
8. If an input is required to be shunted (disabled) for a period of time when the door access function is performed at the reader, program shunt options in “Option 21: Input shunts” on page 171.
9. Ensure that any users who are to perform any access control functions with the reader have an appropriate door group assigned to them. See “Programming users” on page 29.

Using card readers for alarm control

“RAS programming options” on page 89 provide a variety of ways to control the alarm system, depending on the options that are available on the reader. This section describes reader behaviour when various RAS programming options are enabled.

Toggle keyboard control: The [ON] and [OFF] keys lose their function. For arm control the user must present their card followed by [ON], [OFF], or [ENTER]. If a list of areas appears, pressing the area number and [ENTER] toggles the status of the area. If no list appears, the status of the areas is toggled immediately.

Card auto disarms: If the reader has buttons, then the user can arm by presenting the card and pressing the [ON] key. The user can disarm by presenting the card.

Card always disarms/arms and Toggle keyboard control: The user can arm and disarm by presenting the card.

Cards arm after three badges: The user can arm by presenting the card three times within 10 seconds.

Alarm control with key switches

This section provides an overview of the programming steps to enable alarm system control functions to be performed with key switches or other devices wired to a Challenger system input, such as:

- Output contacts from a remote control receiver.
- Output contacts from another security system.
- Push button switch for quick arming on exit (programmed to allow arm but not disarm).

Use the following steps to use an input for alarm control.

1. Plan the system and fill out the programming sheets. See “Planning the system” on page 10.
2. Access the Install menu. See “Accessing the Install menu” on page 18.
3. Program any time zones that may be required in order to limit the alarm control functions of the control input to specific time periods. See “Option 13: Time zones” on page 161.
4. Determine whether an existing alarm group is suitable for the control input. Program a new alarm group if necessary in “Option 5: Alarm groups” on page 96.
    - The alarm group will define the areas and alarm control functions available to the key switch or other device connected to a Challenger input.
    - The special input types used for this purpose require an alarm group to be assigned instead of areas. Alarm groups 11 to 13 are assigned Area Group 1 and may be suitable for key switches, and so on, if all areas in Area Group 1 are to be controlled. Alarm groups 14 to 29 are intended for devices that control a single area.
    - User alarm group option is set to no. Alarm system control option is set to yes.
    - Program other alarm group options as required.
5. Program the input in “Option 1: Input database” on page 70.
6. Determine the number of the input you wish to program. The input numbers allocated for the panel and each DGP address are listed in Table 25 on page 225.
7. Program a suitably descriptive input name.

8. Select one of the “Area Control” input types to suit the purpose of the input (see “Input types” on page 229). For example:
   - Type 6 “Area Control Input - Momentary” for momentary (spring return) key switches, and so on.
   - Type 31 “Area Control Input - Latching: for latching key switches, and so on.
9. Program the input’s alarm group.

Camera control and monitoring

This section provides an overview of the programming steps to control and monitor security cameras and CCTV systems.

Overview

The Challenger system provides the following facilities:

- Eight input types are available for camera frame counting, and eight input types are available for film out reporting (see “Input types” on page 229).
- Camera testing is available utilizing the frame counting feature.
- Special input types are available for suspicion buttons with a timing feature (see “Input types” on page 229).
- The installer can specify which inputs will activate cameras.
- Cameras can also be activated or inhibited via time zones.
- Cameras can be programmed to be activated or inhibited by virtually any event in the system, such as keypad duress, DGP offline, report fail, and so on.
- Camera event flags to activate relays are programmed for each individual area in the system, i.e. inputs can trigger cameras in a single area or in multiple areas.
- Film out is reported to the remote monitoring station in all reporting formats (some formats also report film low).

Programming steps

Use the following steps to control and monitor security cameras.

1. Plan the system and fill out the programming sheets. See “Planning the system” on page 10.
2. Access the Install menu. See “Accessing the Install menu” on page 18.

3. Program the required system options. The options you need to consider for cameras are as follows:
   - "Film low" on page 110. Enter a value greater than 0, even if frame counting is not used.
   - "Film out" on page 110. Enter a value greater than 0, even if frame counting is not used.
   - "Test mode" on page 110. Camera testing facilities are available, which utilize the frame counting feature. To provide automatic camera testing when area 1 is disarmed, select system test option 1 or 3 incorporating the access test.
   - "No. of Relay controllers" on page 111.
   - "Disable 0 [ENTER] for camera reset" on page 117. Set this option to YES if cameras are required to continue operating until the alarm is reset with a PIN.
   - "Financial options" on page 119. Set this option to YES to enable film counts to be displayed as part of camera testing during access test. (Setting this option to YES will also increase the minimum PIN length to 5 digits when programming users).
4. Program any time zones that may be required in order to limit the functions of particular users or arming stations to specific time periods via their alarm groups or to control relays. See "Option 13: Time zones" on page 161.
5. Specify the Camera Event Flag number in the area database for the areas in the system where cameras will be used. See "Option 2: Area database" on page 77. Scroll through the options to locate the Camera Event Flag record.
   - The Camera Event Flag is activated when an input that has the area assigned to it, and the option Camera Event Flag set to YES on the input database, is in alarm.
   - Program an event flag. For convenience you may wish to use the same number as the relay number that will activate the camera.
6. Determine whether an existing alarm group is suitable for camera control or testing. Program a new alarm group if necessary in "Option 5: Alarm groups" on page 96. Ensure that the required menu options are available to the user:
   - Option 5. History
   - Option 6. Test Report
   - Option 8. Film counters
   - Option 13. Start Auto Access Test
   - Option 18. Reset Cameras
7. Program the input in "Option 1: Input database" on page 70. Inputs can be programmed to provide any of the special input facilities for cameras; or as alarm inputs that will activate the cameras.

8. Determine the number of the input you wish to program. The input numbers allocated for the panel or DGPs are listed in Table 25 on page 225.

   Note: Camera frame count inputs can only be connected to the Challenger panel (inputs 1 to 16).

9. Program a suitably descriptive input name.
10. Select one of the input types suited to cameras (see “Input types” on page 229). For example:
    - Type 1 (access alarm) may be used for a holdup button.
    - Type 2 (secure alarm) may be used for motion detector.
    - Type 7 (camera suspicion) input may be used for a camera suspicion button.
    - Type 8 (delayed access/secure alarm) may be used for a hold-up button on a counter where more than one hold-up button is used.
    - Type 9 (reset delayed input) may be used for reset button for quick cancellation of alarm. This input type stops the cameras from operating if the input is unsealed, but the delayed time continues to run. It is used to reset delayed input types 8, 11, 22, and 40.
    - Types 48 to 55 are used to generate a film out alarm.
    - Types 23 to 26 and 36 to 39 are used to increment the camera’s frame count.
11. Program the input’s areas. The camera input must have at least one area assigned. If the input is programmed to activate cameras, only cameras in the areas assigned to the input will be activated.
12. If you need to test the camera, set the input’s test type to 0 (see “Test option” on page 72).
13. If you need the input to activate the siren, strobe, or camera outputs, or if you need the input to activate a relay, then you must assign the appropriate event flags to the input. Set the camera event to YES to enable the input to activate the event flag number specified in the area database for the areas assigned to the input (see “Programming input event flags” on page 73).
14. Program the relevant timers (see “Option 6: Timers” on page 104). In particular, the suspicion time that cameras continue to operate after a suspicion type input (7, 40, and 47) is resealed.
15. If an output is required for a buzzer, lamp, and so on, to indicate the “film out” condition, program the film out event flag (see “Option 34: Program summary event flags” on page 183).
16. Determine the number of the relays you wish to program. The relay numbers allocated for the panel or DGPs are listed in Table 25 on page 225.
17. Program the details for each of the relays in your system that will be used to activate cameras (see “Option 16: Map relays” on page 165)

Programming delayed holdup inputs

This section provides an overview of the programming steps to use the delayed holdup input facilities.

The delayed holdup input types provide a feature which allows holdup or duress type inputs to be activated and generate an alarm locally (activating cameras and other outputs if required), but not report to the remote monitoring station until after a pre-programmed delay has expired. This provides personnel on site the opportunity to rectify the cause and/or reset the alarm if it was activated accidentally or by a faulty input device, before it is reported. If more than one delayed holdup input type is activated, the system will report the alarm instantly.

Use the following steps to program a delayed holdup alarm input type.

1. Determine the holdup button requirements and fill out the programming sheets. See “Planning the system” on page 10.
2. Access the Install menu. See “Accessing the Install menu” on page 18.
3. Program the required system options. The options you need to consider for delayed holdup are as follows:
    - “No. of Relay controllers” on page 111.
    - “Financial options” on page 119.
4. Specify the Pre-Alarm Timer Event Flag number in the area database for the areas in the system where delayed holdup input types will be used. See “Option 2: Area database” on page 77. Scroll through the options to locate the Pre-Alarm Timer Event Flag record.
    - The Pre-Alarm Timer Event Flag is activated when a delayed holdup input that has the area assigned to it, is unsealed. The Event Flag is activated for the delayed period.
    - Program an event flag. For convenience you may wish to use the same number as the relay number that will activate the camera.
    - The Pre-Alarm Timer Event Flag may be used to activate a relay to provide discreet visual indication via a LED, and so on, that the delayed holdup button is active.
5. Program the input in “Option 1: Input database” on page 70.
6. Determine the number of the input you wish to program. The input numbers allocated for the panel and each DGP address are listed in Table 25 on page 225.
7. Program a suitably descriptive input name.
8. Select an appropriate input type to suit the purpose of the input (see “Input types” on page 229). For example:
    - Type 8, “Delayed access/secure alarm” (holdup button)
    - Type 9, “Reset delayed inputs” (button for quick reset & to stop cameras)

- Type 11, “Delayed access alarm” (holdup button)
- Type 22, “Delayed access non-latching/secure alarm” (holdup button)
- Type 40, “Suspicion or delayed access/secure alarm” (special combined suspicion/holdup button)

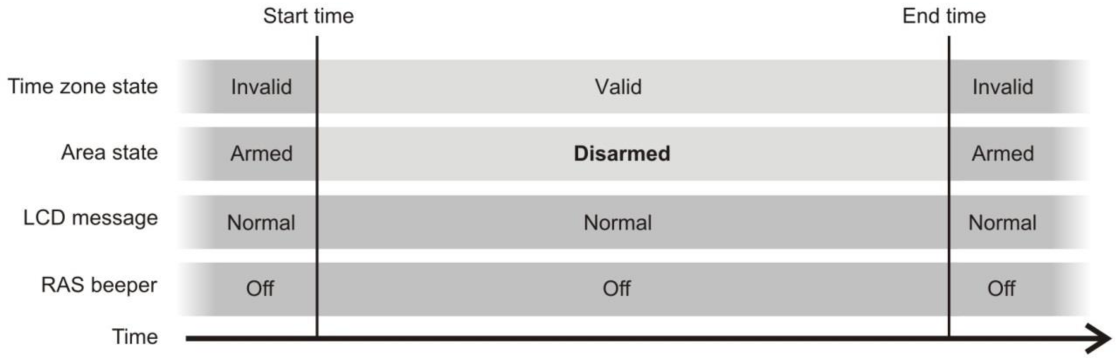
9. If the system is going to report to the Remote Monitoring Station using the Contact ID format, then it is necessary to program a report type for the input. The default type is “140 General Alarm” (sub-class General Alarm).
10. Assign an area or area group to the input that must alarm when the input is unsealed and the area status (secured or in access) meets the requirement for the input type.
    - At least one area must be assigned to an input.
    - Where there is more than one area assigned (via an area group), the input is regarded as being in access if one or more of the areas assigned is disarmed, and in secure only if all the areas assigned are armed.
11. If you selected one of the test options when programming the system options, or if the user wishes to use the access test option in the User menu, then you may need to program a test type for certain inputs. Refer to “Test option” on page 72 for details.
12. If you require the input to activate the siren, strobe, or camera outputs, or if you require the input to activate a relay, and so on, then it is necessary to assign the appropriate event flags to the input. Refer to “Programming input event flags” on page 73.
13. Program timers. The relevant timers for delayed holdup are as follows:
    - “Delay holdup time” on page 105.
    - “Suspicion time” on page 106.
14. Determine the number of the relays you wish to program. The relay numbers allocated for the panel and each DGP address are listed in Table 25 on page 225.
15. Program the details for each of the relays in your system, in “Option 16: Map relays” on page 165. Use the Pre-Alarm Timer Event Flag number that you recorded in the area database for the areas in the system where delayed holdup input types will be used.

Programming automatic arming and disarming

The Challenger system can automatically arm and disarm areas based on a time zone (time of day and day of the week). Time zones are effectively on-off switches (valid or invalid), so an alarm group is also used to define (among other things) the areas that are affected. The time zone and an alarm group are linked via an arm/disarm timer program (see “Option 17: Arm/disarm via TZ” on page 167).

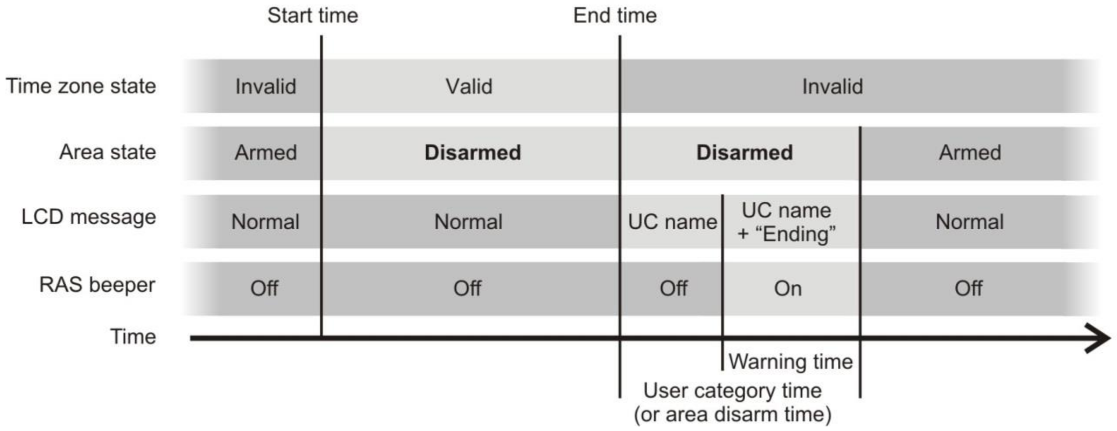
Figure 5 below depicts the effect of the time zone’s state on the area’s armed/disarmed state.

Figure 5: Example of simple arm/disarm timer functionality



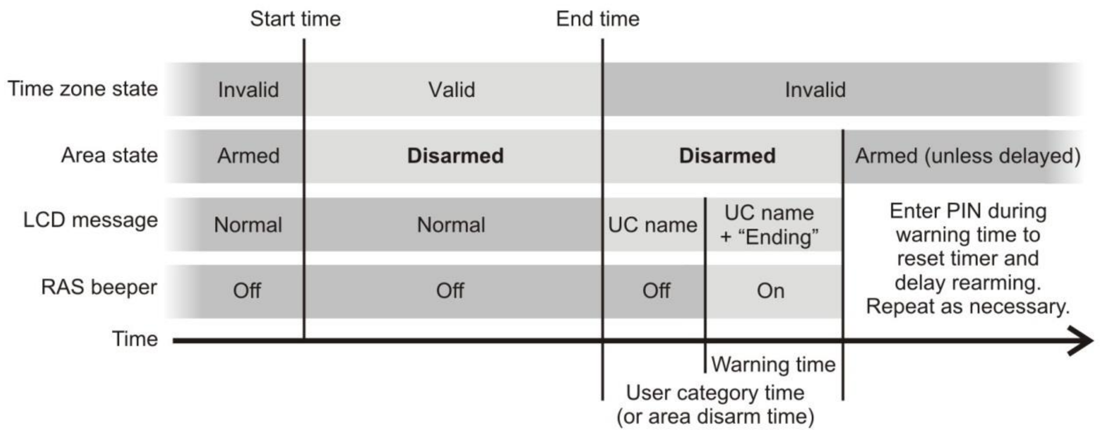
The alarm group can also be linked to a user category in order to provide a warning time, in which the RAS beeper (or other device) sounds to indicate imminent rearming (Figure 6 below).

Figure 6: Example of arm/disarm timer functionality where a user category provides a warning



Users who have the user category in their alarm group can badge or enter their PIN to delay the automatic rearming of areas after the time zone expires (Figure 7 on page 46).

Figure 7: Example of arm/disarm timer functionality where a user can delay rearming



Use the following steps to program automatic arming and disarming.

1. Determine the automatic arming and disarming requirements and fill out the programming sheets. See “Planning the system” on page 10.
2. Access the Install menu. See “Accessing the Install menu” on page 18.
3. Program time zones that will specify the arm and/or disarm times. The time zone must specify both start and end times whether both are used or not. See “Option 13: Time zones” on page 161.
   - The start time will be the time that the areas specified in the alarm group will disarm.
   - The end time will be the time that the areas specified in the alarm group will arm.
4. If a warning prior to arming is required, program a user category so that it can be linked to the alarm group.
5. The alarm group will define the areas and alarm control functions that will be performed when the time zone starts and/or ends. Program the alarm group’s alarm control functions for the area or the area group:
   - If an alarm group is linked to a single area, then the alarm group controls the area’s settings for arming, disarming, alarm reset, and timing (see “Option 5: Alarm groups” on page 96.
   - If an alarm group is linked to an area group (one or more areas), then the area group controls each area’s settings for arming, disarming, alarm reset, and timing (see “Option 36: Area groups” on page 190).
6. The following alarm group options may need to be enabled:
   - Reset system alarms—If “System alarms” on page 117 is enabled, then enabling this option will allow reset of those alarms.
   - Disable auto-deisolate—Enabling this option prevents the alarm group from being able to automatically de-isolate inputs in the areas they disarm.
   - Auto isolate unsealed inputs—Enabling this option allows unsealed inputs to auto-isolate when arming to prevent them causing alarms.

- Forced arming when inputs unsealed—Enabling this option allows areas to arm regardless of any unsealed inputs which may subsequently cause an alarm.
- Prevent forced disarming—Enabling this option prevents areas to be disarmed if there are unsealed inputs (access alarms).

7. Program the alarm group’s time zone to control when this alarm group is valid (the time zone programmed to specify the arm and/or disarm times must not be used here).
   - The “No Timezone” selection specifies the alarm group is always valid and is the typical setting for this application.
   - The time zone could be used in this application to specify particular automatic alarm control functions for a particular time period and then switch to the alarm control functions as specified in the alternate alarm group when the time zone is not valid.
   - If a time zone restriction has been specified for this alarm group, you may assign an alternate alarm group that will take effect when the time zone on this alarm group is not valid.
8. Program the arm and disarm timers in “Option 17: Arm/disarm via TZ” on page 167.

Disarming and arming of common areas

This section provides an overview of how to enable a common area (or areas) to be disarmed and armed according to the status of other areas (for example, a common reception area in a medical suite shared by several practices will disarm when the first practice is disarmed and re-arms when the last practice is armed).

Use the following steps to program common areas.

1. Determine the areas to be considered common and which areas will control the common areas. Fill out the programming sheets. See “Planning the system” on page 10.
   - A common area is an area that will be disarmed and armed automatically according to the status of other specified areas.
   - A controlling area is individually armed and disarmed by the users, but will control the status of the common areas.
2. Access the Install menu. See “Accessing the Install menu” on page 18.
3. Program area linking in “Option 19: Area linking” on page 170.

Programming macros

Overview

A macro logic equation is a tool for activating inputs or event flags based on the conditions of one to four macro inputs (event flags or relays). The macro logic equation can combine macro inputs using AND or OR logic, based on the event flag's or relay's active or inactive (inverted) state. The output of the macro logic equation is an event flag or input.

This section provides an overview of how to program macro logic. See "Option 35: Program macro logic" on page 187.

Use the following steps to program a macro logic equation.

1. Determine the macro logic requirements and fill out the programming sheets. See "Planning the system" on page 10.
2. Access the Install menu. See "Accessing the Install menu" on page 18.
3. Program or determine any event flags required for the macro logic equation. See "Event flags" on page 242.
4. Program or determine any relays required for the macro logic equation. See "Programming relays" on page 30.
5. Program the output of the macro logic equation:
    - If the output of the macro logic equation is an event flag, program the event flag. See "Event flags" on page 242.
    - If the output of the macro logic equation is an input, program the input. See "Option 1: Input database" on page 70.
6. Program a macro logic equation using "Option 35: Program macro logic" on page 187.

Example of macro logic programming

In the following example, we want to prevent door 1 from being unlocked via card reader while door 2 or door 3 is open (for example, airlock doors).

The system is configured in the following manner:

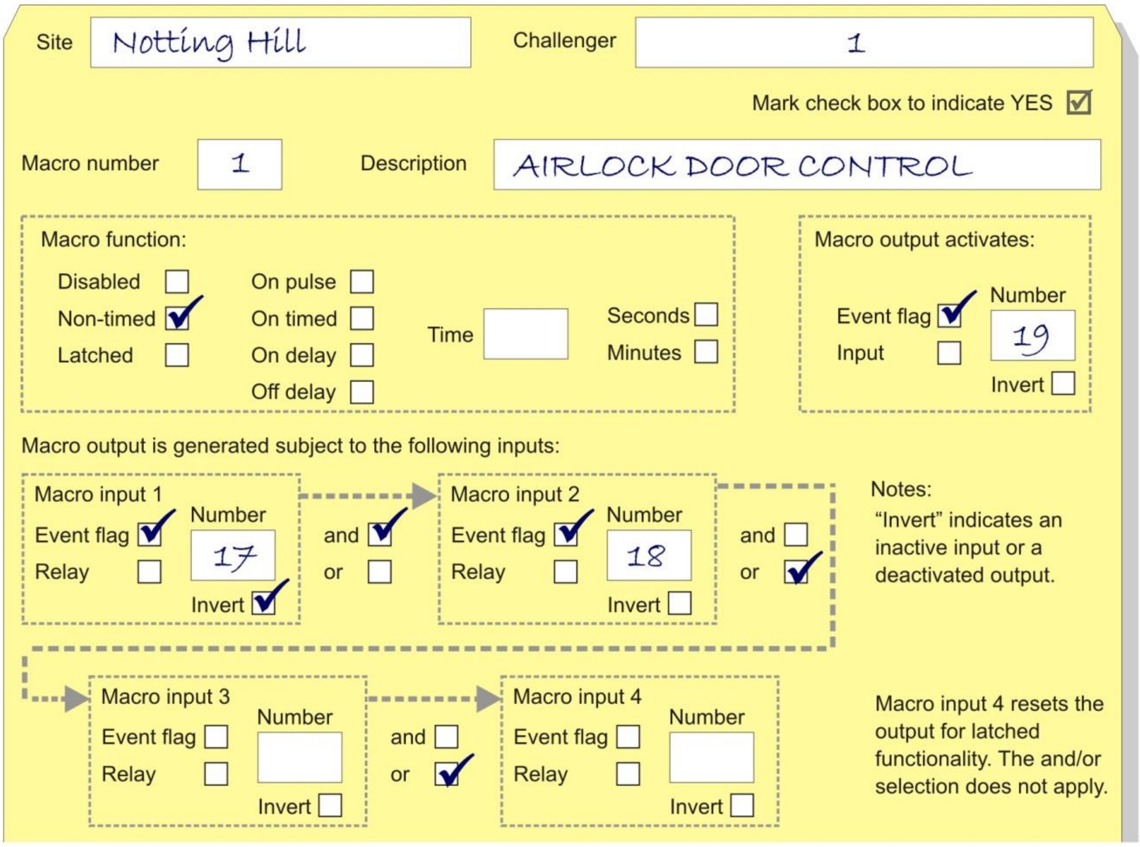
- Contacts on doors 2 and 3 are wired to Challenger inputs 1 and 2.
- Challenger inputs 1 and 2 are programmed as input type 20 (Input to activate event flag 24-hour), and are programmed with event flag 17 as their selected event flag.
- The door 1 reader activates event flag 18 to unlock the door when a valid card is presented.
- The relay that activates the door 1 lock is relay 19 and is mapped to event flag 19.

The macro logic program can be used to ensure that event flag 19 does not activate to unlock the door unless the other two doors are closed.

The logic equation described in Figure 8 below states that event flag 19 will only activate to unlock door 1 if:

- Event flag 17, used for inputs 1 and 2, is inactive (inverted), indicating that neither door 2 or door 3 are open), AND
- Event flag 18 is active (door event flag activated by valid card at reader).

Figure 8: Macro logic worksheet example



Site: Notting Hill   Challenger: 1

Mark check box to indicate YES ☑

Macro number: 1   Description: AIRLOCK DOOR CONTROL

Macro function:

Disabled □   On pulse □
Non-timed ☑   On timed □   Time:
Latched □   On delay □   Seconds □
Off delay □   Minutes □

Macro output activates:

Event flag ☑   Number: 19
Input □
Invert □

Macro output is generated subject to the following inputs:

Macro input 1
Event flag ☑   Number: 17
Relay □
Invert ☑

and ☑
or □

Macro input 2
Event flag ☑   Number: 18
Relay □
Invert □

and □
or ☑

Notes:
"Invert" indicates an inactive input or a deactivated output.

Macro input 3
Event flag □   Number:
Relay □
Invert □

and □
or ☑

Macro input 4
Event flag □   Number:
Relay □
Invert □

Macro input 4 resets the output for latched functionality. The and/or selection does not apply.

When programming macro logic equations via an LCD RAS, the logic equation described in Figure 8 above resembles Figure 9 below. The use of "!" indicates inverted logic.

Figure 9: Macro logic RAS programming example

```
M 1 = !E17 And E18 Or E0 Or E0
*−Chg, Logic 1:
```

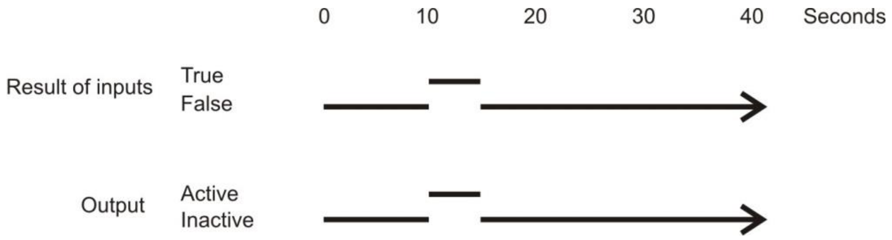
Examples of macro function selections

Macro output functions are listed in Table 18 on page 188. The following sections further describe these options.

Nontimed

Nontimed 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.

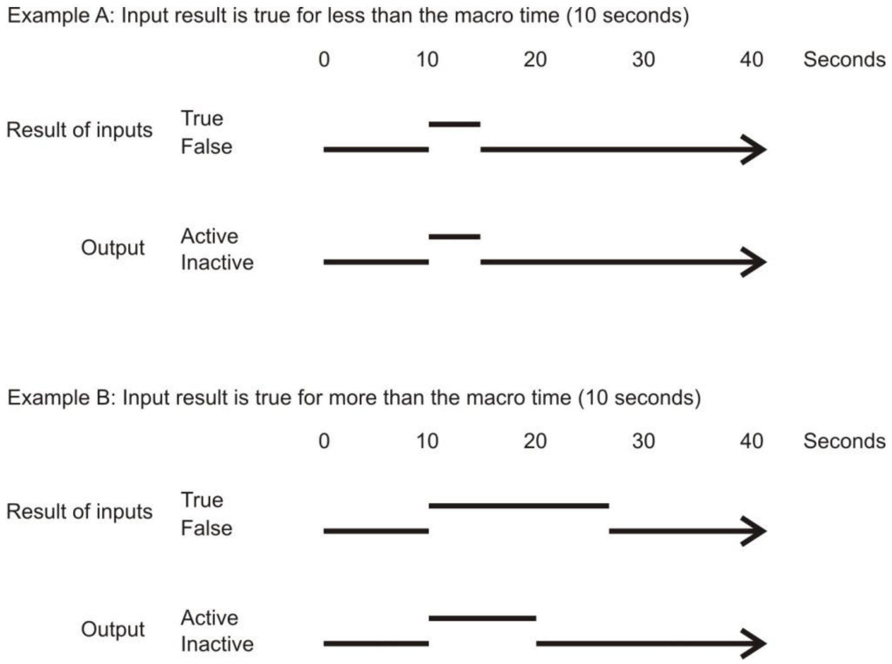
Figure 10: Graphical representation of nontimed macro function



On pulse

On pulse activates for the programmed time or the active period of the logic result, whichever is shortest (Figure 11 below).

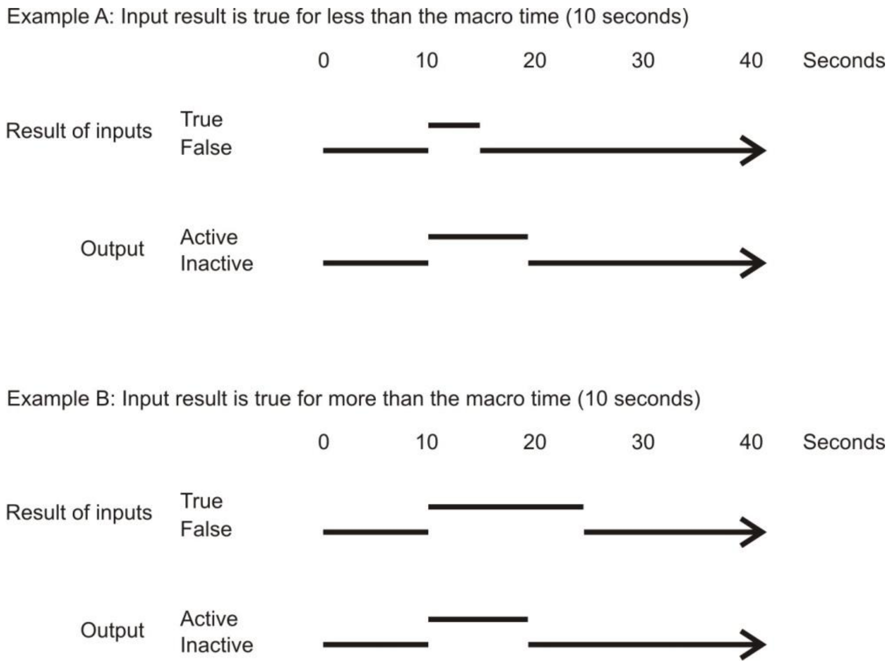
Figure 11: Graphical representation of on pulse macro function


Example A: Input result is true for less than the macro time (10 seconds)
0
10
20
30
40
Seconds
Result of inputs
True
False
Output
Active
Inactive
Example B: Input result is true for more than the macro time (10 seconds)
0
10
20
30
40
Seconds
Result of inputs
True
False
Output
Active
Inactive

On timed

On timed activates for the programmed time regardless of the macro output changing (Figure 12 on page 51).

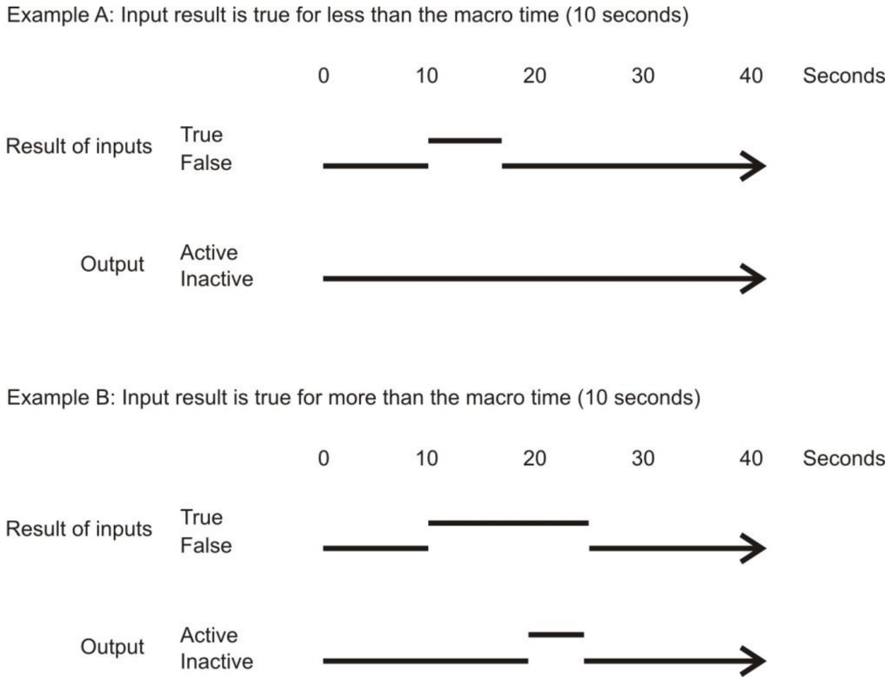
Figure 12: Graphical representation of on timed macro function


Example A: Input result is true for less than the macro time (10 seconds)
0
10
20
30
40
Seconds
Result of inputs
True
False
Output
Active
Inactive
Example B: Input result is true for more than the macro time (10 seconds)
0
10
20
30
40
Seconds
Result of inputs
True
False
Output
Active
Inactive

On delay

On delay activates after the programmed time unless the result of the logic equation is no longer valid (Figure 13 below).

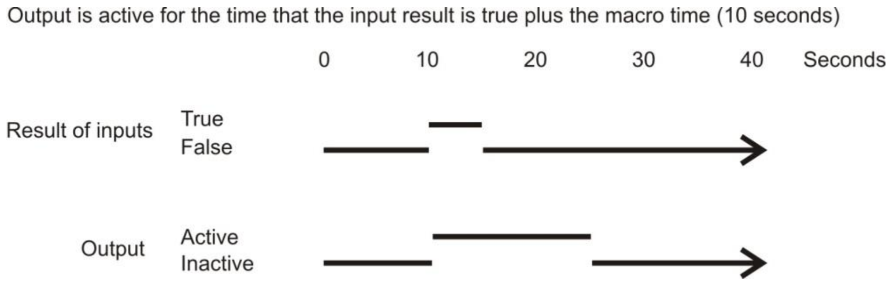
Figure 13: Graphical representation of on delay macro function


Example A: Input result is true for less than the macro time (10 seconds)
0
10
20
30
40
Seconds
Result of inputs
True
False
Output
Active
Inactive
Example B: Input result is true for more than the macro time (10 seconds)
0
10
20
30
40
Seconds
Result of inputs
True
False
Output
Active
Inactive

Off delay

Off delay follows the result of the logic equation, but remains active for the time programmed after the result of the logic equation is no longer active (Figure 14 below).

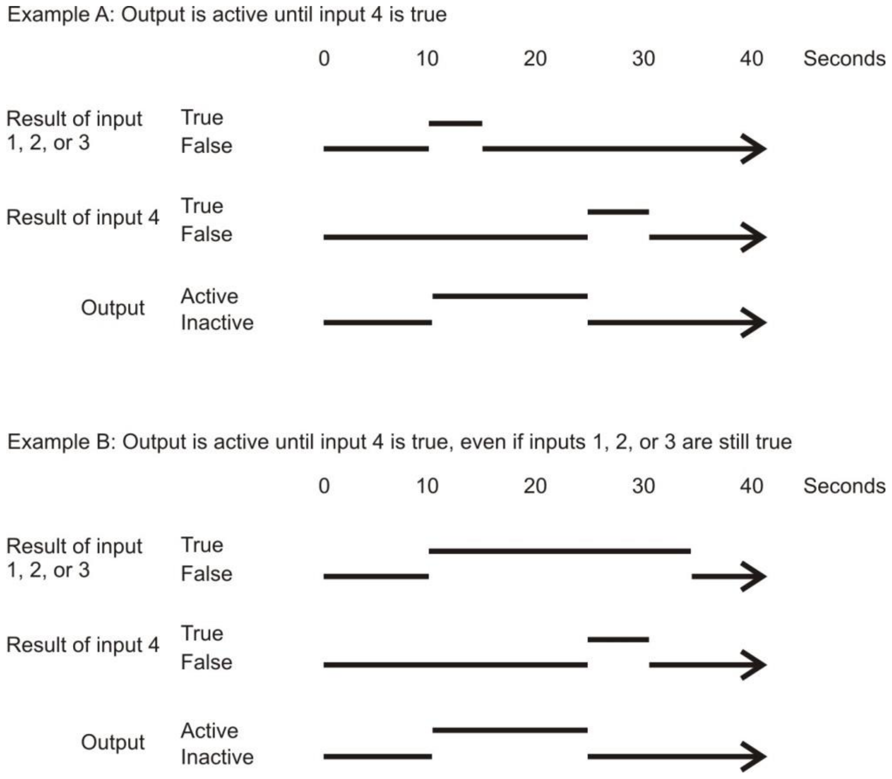
Figure 14: Graphical representation of off delay macro function


Output is active for the time that the input result is true plus the macro time (10 seconds)
0
10
20
30
40
Seconds
Result of inputs
True
False
Output
Active
Inactive

Latched

Latched activates on any of the first three macro inputs in the logic equation and is only reset by the fourth macro input. Any programmed AND / OR function is not used (Figure 15 below).

Figure 15: Graphical representation of latched macro function


Example A: Output is active until input 4 is true
0
10
20
30
40
Seconds
Result of input 1, 2, or 3
True
False
Result of input 4
True
False
Output
Active
Inactive
Example B: Output is active until input 4 is true, even if inputs 1, 2, or 3 are still true
0
10
20
30
40
Seconds
Result of input 1, 2, or 3
True
False
Result of input 4
True
False
Output
Active
Inactive

Programming service technician access

This section provides an overview of the programming required to enable a service technician to access the system functions that they require via a PIN or card, when permitted by an authorised user.

The service technician’s PIN or card is valid only when enabled by a user with the appropriate authority via User menu 17. Enable/Disable Service Technician. Once enabled, the service technician’s PIN or card will remain valid until disabled by a user with the appropriate authority, or the programmed service time expires (see “Option 6: Timers” on page 104).

Enabling the service technician activates the special time zone 25. Time zone 25 is used to enable the service technician’s PIN or card, and can also be used to enable or disable any other system functions, relays, and so on, that are required while the service technician is in attendance.

Use the following steps to program service technician access.

1. Determine the service technician requirements and fill out the programming sheets. See “Planning the system” on page 10.
2. Access the Install menu. See “Accessing the Install menu” on page 18.
3. Ensure that a user (and a RAS) are assigned an alarm group that has access to User menu 17. Enable/Disable Service Technician in order to provide access for the service technician.
4. Program an alarm group suitable for the service technician (the alarm group must have time zone 25 assigned and must not have access to User menu 17. Enable/Disable Service Technician). Program a new alarm group if necessary in “Option 5: Alarm groups” on page 96 and refer to “Alarm group application” on page 97.
5. Program the service time (see “Option 6: Timers” on page 104). When a user enables the service technician, time zone 25 will be valid until the service time expires or until User menu 17. Enable/Disable Service Technician is used to disable the service technician, whichever occurs first.
6. If any relays are required to be held active or inactive when time zone 25 is valid, program the requirements in “Option 16: Map relays” on page 165 (you must know which relays are affected). Assign time zone 25 to the relays.
7. Program the user record that the service technician will use to access the system (as permitted by the alarm group). Refer to “Programming users” on page 29 for details.
8. Program the system to allow service technician access when the system is armed. See “Skip access check for service tech” on page 119.

Triggering console (RAS) beepers

This section provides an overview of the programming required to activate the keypad beeper on any RAS connected to the Challenger system LAN.

The keypad beeper is activated automatically when warning timers are running, local alarms are active, or input test procedures are active. Any input can also be programmed to activate the keypad beeper when in alarm. In addition, the system can be programmed to activate on virtually any type of event or condition that can exist in the Challenger system.

Use the following steps to program a keypad beeper.

1. Determine the keypad beeper requirements and fill out the programming sheets. See “Planning the system” on page 10.
2. Access the Install menu. See “Accessing the Install menu” on page 18.
3. Program an unused event flag number as the Console trigger event flag in “Option 34: Program summary event flags” on page 183.
4. Use the console trigger event flag number in any event flag record for the functions that are to activate the keypad beepers. Event flags are used in many parts of Challenger programming and can be seen on the following programming worksheets:
   - “Input worksheet” on page 251 (selected event flag)
   - “Area worksheet” on page 252
   - “RAS worksheet” on page 254 (door event flag)
   - “Input shunt worksheet” on page 272 (shunt event flag and shunt warning event flag)
   - “Event flags worksheets” on page 274 (all summary event flags)
   - “Macro logic worksheet” on page 277
5. If more than one event is required to activate the keypad beepers, and those events have already been allocated different event flag numbers for other functions, create a macro logic program that will combine the required event flag numbers to activate the console trigger event flag number. See “Programming macros” on page 48 for details.

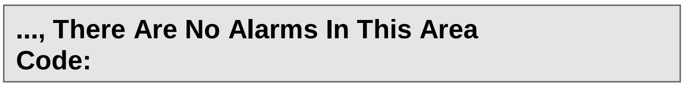
Using keypad duress

An alarm group may be programmed to allow a user to signal a duress condition (for example, a holdup) by entering a special duress code on a keypad RAS (on the Challenger system LAN) instead of their usual door code.

The system will behave as if the user’s PIN was entered (for example, to open a door), and it will initiate a duress alarm. The duress alarm can be reset (cancelled) by entering the normal PIN. Duress codes cannot be used to access a RAS menu (for example, to program the system): a duress code is treated as an invalid code for RAS menu access.

When enabled, the special duress code is the user’s PIN+1 (last digit only). For example, if the user’s PIN is 8914 then the duress code is 8915. If the user’s PIN is 8919, then the duress code is 8910 because only the last digit is affected. When a duress alarm is activated from a keypad connected to the Challenger LAN, the characters “...,” are displayed on the LCD (Figure 16 below).

Figure 16: LCD RAS indication of keypad duress alarm



..., There Are No Alarms In This Area
Code:

To use keypad duress, enable (set to YES) the following options:

- “Keypad duress” on page 100 for the user’s alarm group and the RAS’s alarm group.
- “User alarm group” on page 99 for the user’s alarm group and the RAS’s alarm group.
- The user’s alarm group and the RAS’s alarm group must allow arming and disarming of the applicable areas. If not enabled, the duress code opens the door and activates a duress alarm, but the duress alarm cannot be restored when a normal PIN is entered. Duress can only be reset on a keypad that has alarm system control over at least one area.
- At least one area must be assigned for the RAS’s alarm group. If the RAS is assigned an alarm group without any areas, the duress code opens the door but does not activate or report duress.
- Optionally program a summary event flag to be activated when a keyboard duress alarm occurs. See “Duress event flag” on page 185.

The known limitations of keypad duress are as follows:

- The duress code opens the door but does not activate or report duress if the RAS is programmed for Enter Key Opens Door Only. See “ENTER key opens door only” on page 89.
- When used on a RAS connected to an Intelligent 4-Door or 4-Lift Controller (with duress enabled), a duress code opens the door, regardless of the user’s alarm group and the keypad duress option in the alarm group. The Challenger panel will report the duress alarm; however, there is no way to restore the duress from any door or Challenger RAS, and the RAS on the Challenger LAN do not display “...,” to indicate duress.

Programming common areas

Common areas have inputs that can go into alarm only when all areas are armed (for example, the front door in a building provides an entry to two areas, thus the front door needs to be a common area). There are two ways to create inputs in a common area:

- Assign more than one area (via an area group) to an input. The input can only go into alarm if all areas meet the condition (armed or disarmed). The input is disarmed if one area is disarmed and the longest entry and exit time is used. See “Area or Area Group programming” on page 71.
- Use area linking. The common area is an additional area that automatically secures as soon as the linked areas are secured. See “Option 19: Area linking” on page 170.

The common area can be disarmed separately and has its own entry and exit times. For example, if area 1 is a foyer and is linked to areas 2, 3, and 4, then:

- When any of the linked areas (2, 3, or 4) are disarmed, area 1 will be disarmed.
- When all of the linked areas (2, 3, and 4) are armed, area 1 will be armed.

Linked areas also have control over the common area (if programmed in the alarm group). For example, if area 1 is linked to an area group containing areas 2, 3, and 4, then a user with area 3 can reset an alarm in area 1.

Using Area Search

Area search is a process by which a person must ensure that a facility is safe as part of the disarming process. The following programming is required:

- The person’s alarm group must have area search enabled.
- Minimum and maximum area search times must be defined in Timers.
- An area search time zone must be specified in system options.

Note: The area search time zone must not be a 24-hr time zone because the functionality depends on the time zone changing from valid to invalid to reset the functionality for the next time it is needed. Either soft or ‘hard’ time zones may be used.

Two summary event flags can be used to indicate the state of the area search process:

- Area Search Running
- Area Search Done

The area search process has two modes of operation, depending on whether the Challenger system is configured as a financial institution in System Options or a standard system.

Area search procedure for standard systems (not financial institutions)

The process of disarming via area search is:

1. The person enters the premises when the area search time zone is valid, and disarms the area (or areas). The area search timer starts. During the area search procedure “Area Search” is displayed via LCD RAS.
2. The person searches the premises to determine that there are no threats, and then exits and rearms the premises.

Assuming that the person searched the area, and then exits and rearms the premises between the minimum and maximum area search times, then the premises is deemed to be safe to disarm and enter (open for business).

If rearming occurs before the specified minimum area search time, then an “Area Search Early” alarm is generated (CID 140, point ID 421).

If the area has not been rearmed before the area search timer expires (maximum area search time), then an “Area Search Timeout” alarm is generated (CID 140, point ID 422). The RAS text “Area Search” is replaced with, “..,” until the next time the area is armed or disarmed. After arming or disarming, a “Reset Area Search Failed” message is logged in history.

Area search procedure for financial institutions

The process of disarming via area search is:

1. The person enters the premises when the area search time zone is valid, and disarms the area (or areas). The area search timer starts. During the area search procedure “Morning Check x mins” is displayed via LCD RAS (where x is a countdown of the time remaining starting from the maximum area search time). The area cannot be rearmed until the minimum area search time expires.
2. The person searches the premises to determine that there are no threats, and then exits and rearms the premises.

Assuming that the person searched the area, and then exits and rearms the premises between the minimum and maximum area search times, then the premises is deemed to be safe to disarm and enter (open for business).

If the area has not been rearmed before the area search timer expires (maximum area search time), then an “Area Search Timeout” alarm is generated (CID 140, point ID 422). The RAS text “Morning Check x mins” is replaced with, “..,” until the next time the area is armed or disarmed. After arming or disarming, a “Reset Area Search Failed” message is logged in history.

Configuring IP connections

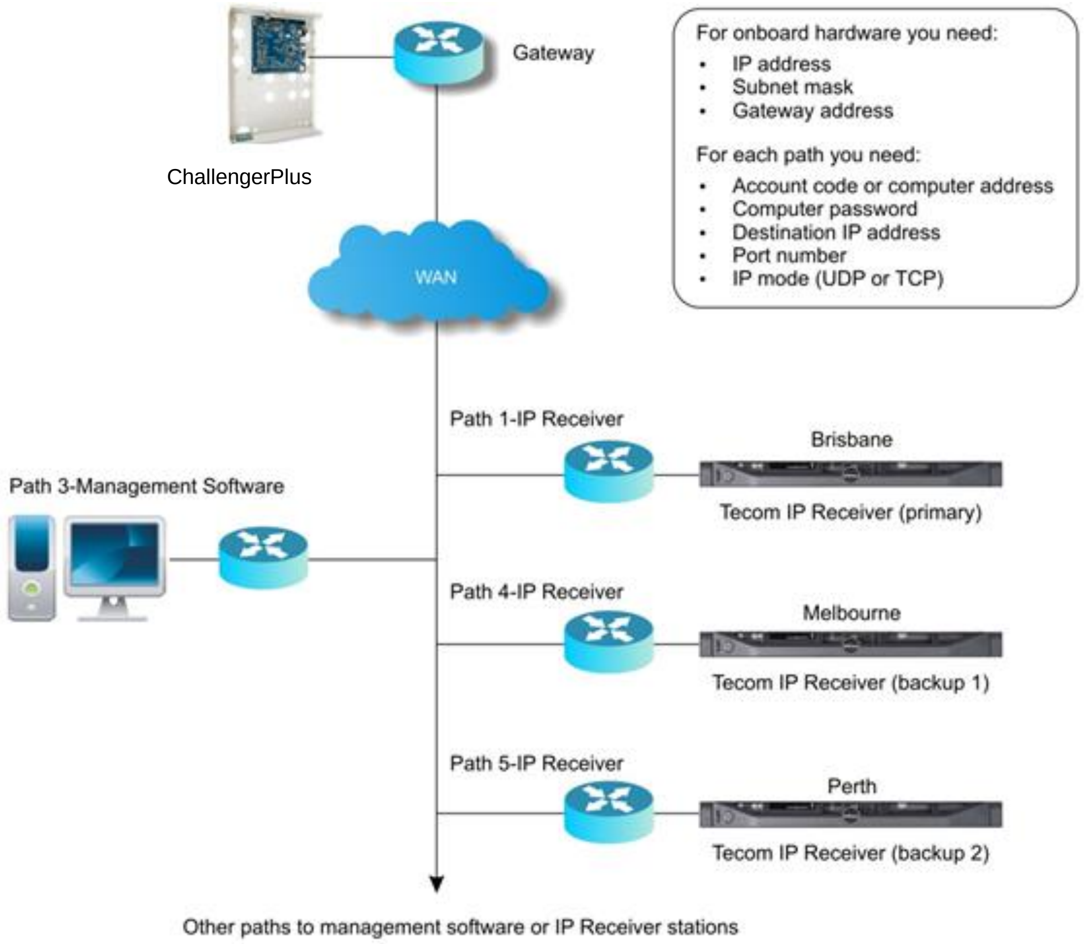
Overview

Challenger panels have native Ethernet support and can communicate with remote computers via one or more of 10 communications paths. Refer to “Setting up communications paths” on page 129 for additional details.

WARNING: Configuring IP communications requires consultation with the client’s Network Administrator. Failure to gain the essential information from the client may result in the Challenger panel not communicating with the IP Receiver, management software, or introducing data collisions with parts of the client’s existing IP network and possibly a total network shutdown.

Figure 17 below is an example of how the Challenger panel’s Ethernet port can be used for simultaneous connection to multiple computers.

Figure 17: Overview of IP connectivity



Migrating from Challenger V8

Challenger V8 panels use an Ethernet interface module such as TS0099 to provide an IP connection. This section describes where to find the settings you need.

Table 4 below lists the required programming items, and their locations in both Challenger*Plus* and Challenger V8 RAS menu structures.

Table 4: IP-related programming items and where to find them

Item	Challenger*Plus* path	Challenger V8 path
Challenger IP address	Communications > Hardware > Onboard > IP address	Extended Protocol Configuration > Challenger IP address
Challenger gateway address	Communications > Hardware > Onboard > Gateway address	Extended Protocol Configuration > Gateway (Router) IP address
Challenger subnet mask	Communications > Hardware > Onboard > Subnet mask	Extended Protocol Configuration > Host bits
Enable hardware	Communications > Hardware > Onboard > Enable Ethernet	Extended Protocol Configuration > Enable TCP/IP UDP/IP support
Path number	Communications > Path > Enter Comm Path	Not applicable
Path format	Communications > Path > Path Main > Format	Not applicable
Enable path	Communications > Path > Path Main > Enabled	Not applicable
Path location	Communications > Path > Path Main > Location	Not applicable
Path slot	Communications > Path > Path Main > Slot	Not applicable
Account code or computer address	Communications > Path > Path Main > Account Code	Communications > Computer address
Security password	Communications > Path > Path Main > Computer Password	Computer Connection > Security Password
Destination IP address	Communications > Path > Path IP Address > IP Address	Extended Protocol Configuration > Contact ID Station IP address (up to 3) Extended Protocol Configuration > Management software IP address (up to 2)
IP port number	Communications > Path > Path IP Address > Send IP Port and Listen IP Port	Extended Protocol Configuration > Challenger IP port

Item	Challenger*Plus* path	Challenger V8 path
IP mode (UDP/IP)	Communications > Path > Path IP Address > IP Mode	Extended Protocol Configuration > Enable Extended Event protocol
Encryption type	Communications > Path > Path Encryption Settings	Not applicable
Encryption keys	Communications > Path > Path Encryption Settings	Communications > Encryption key
Heartbeat	Communications > Path > Path Advanced Settings > Heartbeat Timeout	Extended Protocol Configuration > Heartbeat Timeout
Acknowledgement timeout	Communications > Path > Path Advanced Settings > Timeout	Extended Protocol Configuration > Event Ack Timeout

Advanced network administration

Enterprise-scale sites may have network security measures in place that need to be considered when configuring Challenger IP communications.

For example, the Challenger panel may be configured to communicate with various devices (on various communications paths) over the “Send IP Port” and the “Listen IP Port” which might both be programmed as port 3001. However, the customer’s network might be configured to block communications based on source ports (also known as local ports).

Source or local IP port assignment

Source ports are assigned by the Challenger panel for each communication path that is configured for IP communication.

The source port for a communication path is assigned when the communication path establishes a connection with its configured destination (or re-establishes communication any time the panel restarts).

When the first IP connection is established, the path’s programmed Send IP Port number (for example, 3001) is used as the source port number.

The source port numbers assigned to any subsequent IP connections start at port 4999 and count down (4998, 4997, and so on, to 1024).

For example, on a Challenger panel:

- Communication path 3 is configured to communicate with CTPlus on Send IP Port 3002.
- Communication path 4 is configured to communicate with the primary Tecom IP Receiver on Send IP Port 3001.
- Communication path 5 is configured to communicate with the secondary Tecom IP Receiver on Send IP Port 3001 (Tecom IP Receiver requires the port number to be 3001).

If each of the communication paths connect to their destinations in the order shown above, then the assigned source port numbers would be 3002, 3001 and 4999, respectively.

Using timed input testing

Various options for testing security devices (inputs) are described in the *ChallengerPlus Administrators Manual*. This section describes the programming required to configure the Challenger panel to use timed input testing.

Past versions of Challenger panels allowed inputs to be tested (typically unsealed and then resealed) in the following situations:

- On an ad hoc basis when a device appears to be faulty
- During an access test (a timed interval that starts when areas are disarmed)
- During a secure test (a timed interval that starts when areas are armed)

Challenger*Plus* panels allow inputs to be tested during normal operation within a specified number of days and will report an alarm for inputs that haven’t been tested.

For example, a sensor that is normally activated on a daily basis would be considered to be successfully tested in normal operations. However, a sensor in a room that gets little traffic could be programmed to be tested within seven days so that if a week passes without the sensor being activated, then an input test failed message (CID 307 ‘Self-test failure’) is generated for the input number.

During access tests and secure tests, the Challenger panel’s LCD RASs lists all untested inputs, and removes inputs from the list as they are tested. The list includes inputs that are programmed for timed input testing, and removes these from the list, even if tested during normal operation (outside of access or secure tests).

Inputs that are programmed for timed input testing have a testing interval timer (for example, 30 days). The timer is reset and the input is considered as untested each time the testing interval expires.

To program timed input testing:

1. Enable the System option “Enable expanded test reporting” on page 119.
2. For each input to be timed, select option 2 “Tested in Secure Test & Access” in “Test option” on page 72.
3. For each input to be timed, specify the testing interval in “Test input within no. of days” on page 75.
4. If you need to time only on certain days of the week (defined by a time zone), then use “Decrement test days during TZ” on page 114 to assign the time zone.

5. Optional: After programming time input testing, reset the timer to 0 before handing over to the customer. See “Option 38: Reset input test days” on page 193.
6. Optional: When an input is tested within its specified number of days, you can send a test success message for the input number. See “Expanded test success reporting” on page 120.

Programming text via RAS

Many entities, such as inputs, areas, and so on, can be programmed with a names to identify them. The initial RAS display for input 1 is shown below.

```
1:
(1)−Edit
```

Press 1 to add (or overwrite) text and numbers via RAS (see Table 5 below). The name may contain up to 30 characters (including spaces).

```
1: ,(*)−End
10 Ferntree Place, front door PIR_
```

When each required character is displayed, press [ENTER] to move the cursor to the next position (and to save the characters to the left of the cursor). When finished, press * to save the programming.

Table 5: Key press to get character

Key	1st	2nd	3rd	4th	5th	6th	7th
1	A	B	C	1	a	b	c
2	D	E	F	2	d	e	f
3	G	H	I	3	g	h	i
4	J	K	L	4	j	k	l
5	M	N	O	5	m	n	o
6	P	Q	R	6	p	q	r
7	S	T	U	7	s	t	u
8	V	W	X	8	v	w	x
9	Y	Z	sp	9	y	z	sp
0	.	—	&	0	.	—	&

If the item already has a name (as shown below), and you want to completely delete it, use the following steps.

```
1: 10 Ferntree Place, front door PIR
(1)−Edit
```

Press 1 to begin editing. Note the flashing cursor below the first character.

```
1: 10 Ferntree Place, front door PIR ,(*)−End
10 Ferntree Place, front door PIR
```

Press [0] to replace the first character with a “.” (see Table 5 on page 62).

```
1: 10 Ferntree Place, front door PIR ,(*)−End
.Ferntree Place, front door PIR
```

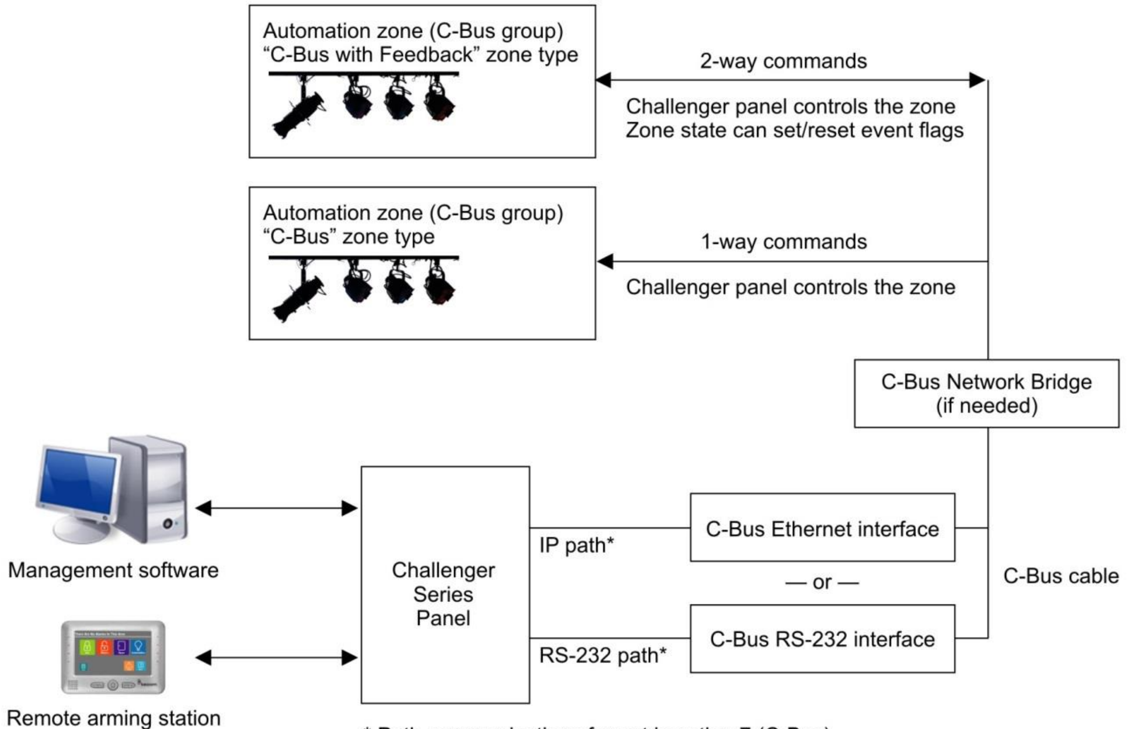
Press * to delete all characters and save the programming.

Automation overview

An automation zone is one or more building devices (including C-Bus® devices) that can be controlled by the Challenger panel via a system RAS or via supported management software or remote devices.

Figure 18 below is a general overview of the relationship between a Challenger panel and two automation zones (C-Bus groups).

Figure 18: Automation overview diagram



* Path communications format is option 7 (C-Bus)

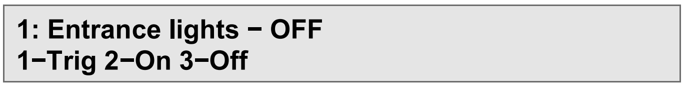
Automation zones are programmed in “Option 39: Automation” on page 193. Refer to “Controlling automation zones via RAS” below for details about manually turning automation zones on and off via an LCD RAS.

Controlling automation zones via RAS

Subject to the automation zone’s programming, a RAS can be used to manually control the zone by activating it, or by immediately turning it on or off.

Figure 19 below depicts the RAS display for automation zone 1 named “Entrance lights”.

Figure 19: Automation zone control screen



1: Entrance lights − OFF
1−Trig 2−On 3−Off

The top line indicates the current state of the zone. Press a number to perform the following actions:

- Press [1] to trigger the automation zone according to its programming. Press [1] again, or press [MENU*], to update the RAS display.
- Press [2] to turn the automation zone on immediately at 100% until turned off or triggered (in which case the zone’s programming will turn it off).
- Press [3] to turn off (reset) the automation zone.

Refer to “Control via User menu” below, “Control via Quick Control” below, and “Control via Install menu” on page 65 for the required programming.

Control via User menu

The relevant programming for controlling automation zones via the User menu 24–Automation Control includes the following items:

- There must be at least one RAS designated to control the zone in “Control zone on RAS” on page 197. If one RAS is designated, then the automation zone can be controlled by a user at only that RAS.
- At least “Enable manual control” on page 196 must enabled. If this option is enabled by itself (manual on control and manual off control disabled), then the user can select only RAS option “1–Act” to activate (trigger) the zone.
- If the option “Manual on control” on page 196 is also enabled, then the user can also select RAS option “2–On” to turn the zone on immediately at 100%.
- If the option “Manual off control” on page 197 is also enabled, then the user can also select RAS option “3–Off” to turn the zone off immediately.

Refer to the *ChallengerPlus Administrators Manual* for details about the User menu.

Control via Quick Control

Quick control uses the CA111x RAS’s multi-function key as a shortcut to the automation zone control screen (Figure 19 above).

Note: Quick control does not require user authentication via PIN. We recommend that control be assigned to a specific RAS (in a secure area) in “Control zone on RAS” on page 197 in order to prevent unauthorised use.

The relevant programming for controlling automation zones via quick control includes the following items:

- There must be at least one RAS designated to control the zone in “Control zone on RAS” on page 197. If one RAS is designated, then the automation zone can be controlled by a user at only that RAS.
- At least “Enable quick control” on page 196 must be enabled. If this option is enabled by itself (manual on control and manual off control disabled), then the user can select only RAS option “1–Trig” to trigger the zone.
- If the option “Manual on control” on page 196 is also enabled, then the user can also select RAS option “2–On” to turn the zone on immediately at 100%.
- If the option “Manual off control” on page 197 is also enabled, then the user can also select RAS option “3–Off” to turn the zone off immediately.

Control via Install menu

Regardless of an automation zone’s programmed control options, an installer can use via the Install menu 43–Automation Status to select RAS option “1–Trig” to trigger the zone.

The following items allow additional control:

- If the option “Manual on control” on page 196 is enabled, then the installer can also select RAS option “2–On” to turn the zone on immediately at 100%.
- If the option “Manual off control” on page 197 is also enabled, then the installer can also select RAS option “3–Off” to turn the zone off immediately.

Refer to the install menu “Option 43: Automation status” on page 200 for details.

Programming twin trip inputs

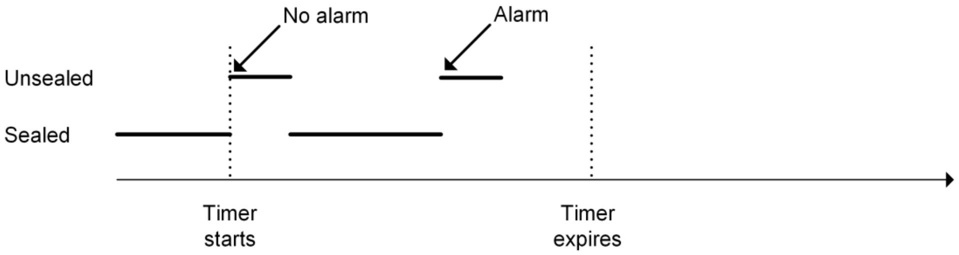
It may sometimes be necessary to allow an input to be briefly unsealed without generating an alarm immediately. In this case, the input can be designated as a **twin trip** input. Twin trip inputs will not generate an alarm if they are unsealed (i.e. tripped) and then re-sealed only once within a specified amount of time (the maximum twin trip time).

A twin trip input will not generate an alarm immediately when it is unsealed and all assigned areas are armed. Instead, it will start a twin trip timer, which runs for the maximum twin trip time.

Note: A maximum of five twin trip timers can run simultaneously. If a twin trip input is unsealed and all five twin trip timers are already running, then the input will generate an alarm immediately.

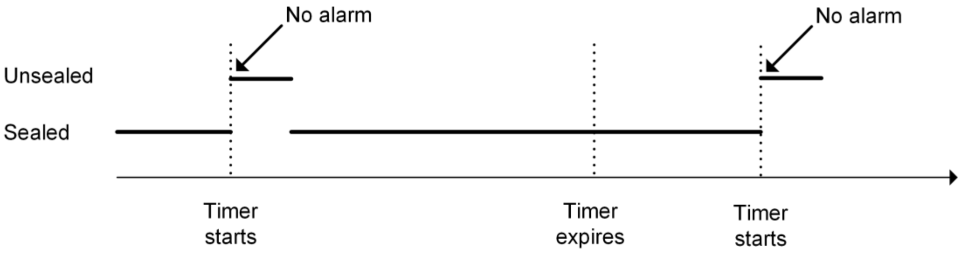
If a twin trip input is unsealed a second time whilst its twin trip timer is running, then it will generate an alarm:

Figure 20: Twin trip input unsealed before timer expiry



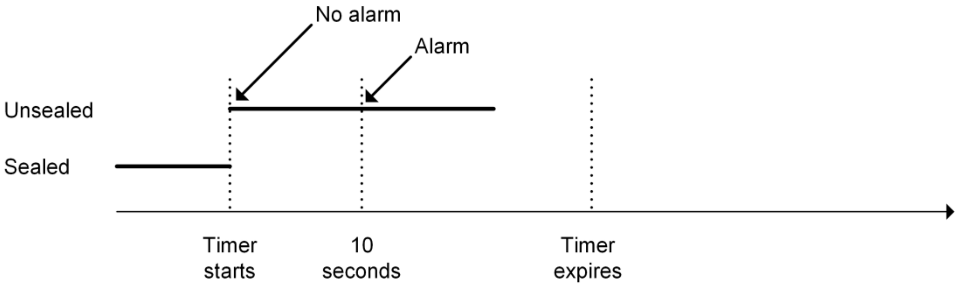
If a twin trip input is unsealed a second time after the twin trip timer has expired, then a new twin trip timer is started (if available) and the input will not generate an alarm:

Figure 21: Twin trip input unsealed after timer expiry



If a twin trip input remains unsealed for longer than 10 seconds then it will generate an alarm:

Figure 22: Twin trip input unsealed for 10 seconds



If a twin trip timer is running and another input (which does not have a twin trip input type) is unsealed in the same area, then both inputs will generate an alarm immediately.

If a twin trip timer is running and another twin trip input is unsealed (whether the second input is in the same area or not), then another twin trip timer will be started (if available). Thus, both twin trip inputs will run a timer and wait for a second unseal before generating an alarm.

If a twin trip input is unsealed when another input in the same area is already in alarm and all assigned areas are armed, then the twin trip input will generate an alarm immediately.

A “twin trip timer started” event will occur when any twin trip timer is started. The event will carry the number of the input that started the timer.

An input can be designated as a twin trip input by setting its input type to one of the following:

- Twin trip secure alarm (input type 60)
- Twin trip entry exit handover (input type 61)
- Twin trip handover no seal check (input type 62)

See “Input type” on page 70 for instructions on programming the input type of an input.

The maximum twin trip time is configured in “Option 6: Timers” on page 104.

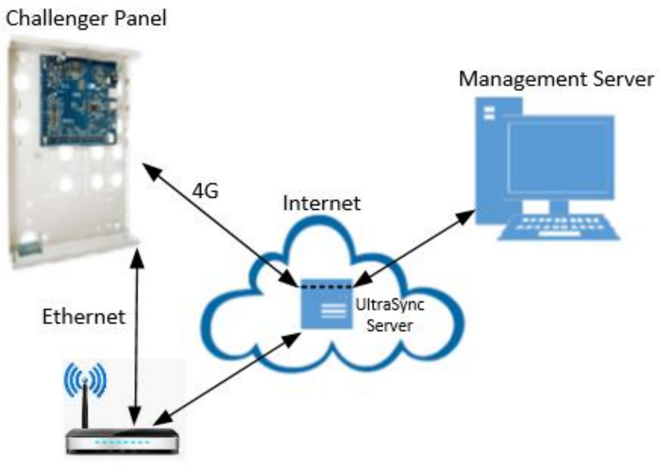
Connecting via UltraSync

Overview

ChallengerPlus panels support **UltraSync** communication. UltraSync provides a secure cloud connection between the Challenger panel and management software or monitoring station using an Ethernet and/or 4G connection through the Internet as shown in figure 23 below.

For further information, please refer to the *UltraSync Configuration Guide* document.

Figure 23 UltraSync Connection



Chapter 5
Command reference

Summary

This chapter describes the Install menu commands that can be performed from an LCD RAS on the Challenger system LAN.

The Challenger system may contain Intelligent Access Controllers, which have local LANs and their own command structure. In addition, the system may be operated from management software, which also has its own command structure. The details provided in this chapter pertain to the commands that can be performed on the Challenger system LAN via an LCD RAS.

- If using an Intelligent Access Controller, refer to its programming manual for programming details.
- If using management software, refer to its user guide or online help for programming details.
- For Challenger User menu commands (for example, to program users) refer to the *ChallengerPlus Administrator’s Manual*.

Content

Option 1: Input database

Each input is a physical input on the control panel, a DGP, or a plug-in expander. Alternatively, an input can be the output of the macro logic equation (see “Option 35: Program macro logic” on page 187).

A worksheet is provided to record programming details and to further describe this option. See “Input worksheet” on page 251.

Input number

Select the appropriate input number to program.

```
Input Database
Input:
```

Every input has a number in the range 1 to 1008, depending on the location in the system.

Enter the input number to be programmed, and then press [ENTER].

Input name

Program a name to identify the input (for example, when an alarm has occurred).

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Input type

Enter the input type number (see Table 28 on page 231) and then press [ENTER].

```
1: Type 2, Secure Alarm
Type:
```

The input type determines exactly how the input will function in given circumstances.

Note: The input type is important and influences much of the programming and functions of the system. You must be very careful when programming input types. All inputs used for safe or vault monitoring must be a 24-hour alarm input type.

Reporting of input

Use this option to select the Ademco Contact ID (CID) message to be reported to the monitoring company if the input or the system generates an event. The details of the data sent to the monitoring company depend on the reporting format.

The example shows the default report ID type for input 1 as number 25. Option number 25 corresponds to the Ademco Contact ID event class “140 General Alarm” (sub-class General Alarm). The sub-class is not displayed on the RAS.

```
1: 25−140, General Alarm
Report ID:
```

Enter a report ID number in the range 1 to 57, and then press [ENTER].

See “TS-CHPLUS CID CODES” excel sheet for a list of CID codes by report ID number. If reporting CID events for inputs, system events are also reported.

Note: Input numbers in the range 1000 to 1008 will not report CID alarms.

Area, area group, or alarm group assignment

An area, an area group, or an alarm group must be linked to the input. The option displayed on the RAS depends on the input type specified for this input.

Refer to the following sections:

- For most input types, refer to “Area or Area Group programming” below.
- For input type 9 (reset delayed inputs), and area control input types 6, 31, 34 and 35, refer to “Alarm group programming” on page 72.

Area or Area Group programming

Except for area control input types, you must assign an area or an area group to the input so that the input can generate an alarm when the input is unsealed and the area status (secured and/or in access) meets the requirement for the input type.

Note: At least one area must be assigned to an input. It is not possible to reset an alarm on an input without an area assigned.

Area groups are used to assign multiple areas to an input. This is typically used:

- To program an additional area that is designated to have overriding control over the alarm functionality for this input. See “Total disarm” on page 108.
- To create a common area. Common areas have inputs that can go into alarm only when all areas are armed. See “Programming common areas” on page 56.

Figure 24: Area or Area Group programming (area mode)

```
1: Area 1
'*'−Grp, Area:
```

If the bottom line displays "'*'-Grp, Area:" (Figure 24 on page 71), then enter an area number in the range 1 to 99 to assign an area to the input, and then press [ENTER].

Alternatively, press [*] to assign an area group to the input Figure 25 below.

Figure 25: Area or Area Group programming (area group mode)

```
1: Area Group 0
'*'−Chg, Grp:
```

If the bottom line displays "'*'-Chg, Grp:" (Figure 24 on page 71), enter an area group number in the range 1 to 255 to assign an area group to the input, and then press [ENTER].

To remove a programmed area or area group, press [0] [ENTER] when prompted for the area or area group number.

Alarm group programming

```
Input: 1 Alm−Grp: 2−Master RAS or Door
Alm−Grp
```

Alarm groups are assigned to inputs that reset delayed inputs or perform alarm control. Alarm groups are only available for input type 9 (reset delayed inputs), and area control input types 6, 31, 34 and 35 (see Table 28 on page 231).

Area control inputs are used to arm/disarm areas (they cause the input to act like a user entering an alarm control code).

Enter the area or alarm group numbers to be assigned to the input being programmed, and then press [ENTER].

Test option

The test option value defines the behaviour of this input during a secure test or an access test (input testing interval). Refer to "Testing Input Devices" in *ChallengerPlus Administrator's Manual* for details.

```
1: 0, No Testing Required
Test Type:
```

Enter a number for the test type (see Table 6 below) and then press [ENTER].

Table 6: Input Test Types

Number	Test type	Description
0	No Testing Required	The alarm input is not programmed to be tested during either a secure test or an access test. Select this test type for camera count input types for cameras to be tested during an access test. Example: A button that is active during test mode, siren cover, and panel tamper.

1	Test During Access Test	The input is programmed to be tested during the access test, and is disabled during the access test. Example: Hold-up button.
2	Tested in Secure Test & Access	The input is programmed to be tested during the secure test, and is considered to be already tested if the input's state is toggled from sealed to unsealed, and then back to sealed during access. Example: PIR detectors, doors.
3	Test During Secure Test	The input is programmed to be tested during the secure test. Example: To enable you to test a door contact at the end of the day when arming the area.
4	Set Event Flag 13 During Access Test	The input has event flag 13 during the access test. This test type is used for testing devices activated by access alarm input types (e.g. holdup buttons). The device must already be programmed to be activated by access alarm event flag 13.
5	Set Pre-Alarm During Access Test	The input activates the - event flag during the access test in the areas assigned to the input. This test type is used to test devices that are activated during the delayed hold-up time. The pre-alarm event flag number is programmed in the area database.

Note: During the secure test, the tester event flag (event flag 16) will be activated during half the tester event flag time. Use this event flag to activate devices to generate alarms. The other half of the tester event flag time is used for the device to switch back to sealed state.

See also “Test mode” on page 110 for related programming.

Programming input event flags

An input can have multiple event flags assigned to it, including one event flag assigned by number and pre-defined event flags (YES/NO values). Event flag numbers from 1 to 16 are the system’s predefined event flags, and numbers from 17 to 255 are programmable event flags. Refer to “Event flags” on page 242 for details.

Not all input types can activate event flags. Refer to “Input types” on page 229 for details.

The event flags that can be programmed for an input are described in the following sections.

Input event flag

Assign the optional custom event flag.

```
1: No Event Flag For Input
Event Flag:
```

Enter a number in the range 1 to 255 for the “selected event flag” to be activated at any time an alarm is generated by the input. It is typically used wherever an indication of individual input status is required.

Siren event

Program the siren event flag number in the area database for each of the areas that activate sirens and that are assigned to the input.

```
1: YES − Siren Event, Program in Area DB
*−Change 0−Skip
```

YES The siren event flag specified in the area database is activated when the input generates an alarm, and all the areas assigned to the input are armed.

NO The siren event flag will not be triggered by an alarm in this input.

Console warning

```
1: NO − Console Warning
*−Change 0−Skip
```

YES When the input activates an alarm, the console warning (keypad buzzer) is activated on the keypads that control the areas assigned to the input.

NO An alarm on the input will not trigger the console warning.

Make all events 24-hour

This option causes any event flags assigned to the input to be active when the input generates an alarm, regardless of the secure or access status of the area. For example, the client may want the siren and strobe to activate during the day if the input wiring is tampered or damaged.

```
1: NO − Make All Events 24-Hour
*−Change 0−Skip
```

YES All event flags are triggered when the input generates an alarm, regardless of the secure or access status of the area.

NO The event flags are triggered depending on the secure or access status of the area assigned to the input.

Secure alarm (event flags 2, 3, 4, 5, 9, 10, and 11)

```
1: YES − Event Flag 2, Secure Alarm
*−Change 0−Skip
```

YES The event flag is triggered when the input generates an alarm and the area is secure.

NO The event flag is not triggered.

Access alarm (event flags 6, 7, and 13)

```
1: NO − Event Flag 6, Access Alarm
*−Change 0−Skip
```

YES The event flag is triggered when the input generates an alarm and the area assigned to the input is in access.

NO The event flag is not triggered.

24-hr alarm (event flag 8)

```
1: NO − Event Flag 8, 24-Hr Alarm
*−Change 0−Skip
```

YES The event flag is triggered when the input generates an alarm, regardless of the status of the area assigned to the input.

NO The event flag is not triggered.

Activate selected event on unseal

```
1: NO − Activate Selected Event on Unseal
*−Change 0−Skip
```

YES The selected input event flag (programmed in “Input event flag” on page 73) is triggered when the input changes from sealed to unsealed, regardless of the status of the area assigned to the input.

NO The input event flag is only triggered when the input generates an alarm.

Note: Not applicable to input types 0, 6, 9, 10, 12, 17, 19, 23, 24, 25, 26, 31, 33, 34, 35, 36, 37, 38 or 39.

Camera event

Program the event flag number in the area database for each of the areas that have cameras that are assigned to the input.

```
1: NO − Camera Event, Program in Area DB
*−Change 0−Skip
```

YES The camera event flag programmed in the area database is activated whenever the input generates an alarm.

NO The camera event flag will not be triggered.

Print input when unsealed

```
1: NO − Print Input When Unsealed
*−Change 0−Skip
```

YES Each time the input changes from sealed to unsealed a message is sent to the printer or computer, as applicable.

NO Changes from sealed to unsealed are not printed or sent to a computer.

Note: Door open and close messages may also be sent for shunted inputs.

Test input within no. of days

```
1: Test Input Within: 0
No Days
```

Inputs that are programmed as “Test During Access+Secure” test type, can be assigned a timer (number of days). If the input hasn’t been tested within the specified number of days, then the input reports a ‘Self-test failure’ alarm.

The input may be tested during an access test, a secure test, or as the result of normal operation outside of the test times. See “Using timed input testing” on page 61 for details.

Enter a number of days in the range 0 to 255 for the input’s testing timer.

Notes:

- Use a sufficiently large number of days to accommodate times when there will be no activity, such as weekends or holidays.
- This functionality requires the System Option “Expanded Test Reporting” to be enabled. (The System Option “Test Mode” is not relevant.)

Second event flag

Assign an optional second event flag to be triggered when the input is unsealed, isolated, or in alarm (as determined by the next three options).

```
1: Second Event Flag is 0
E/F No:
```

Enter a number in the range 1 to 255 for the second event flag.

Unsealed triggers second event flag

When enabled, the event flag programmed in “Second event flag” above is triggered when this input is unsealed.

```
1: NO − Unsealed Triggers Second E/F 0
*−Change 0−Skip
```

YES The event flag is triggered when the input is unsealed (regardless of the status of the area assigned to the input).

NO The event flag is not triggered by this condition.

Note: Not applicable to input types 0, 6, 9, 10, 12, 17, 19, 23, 24, 25, 26, 31, 33, 34, 35, 36, 37, 38 or 39.

Isolate triggers second event flag

When enabled, the event flag programmed in “Second event flag” above is triggered when this input is isolated.

```
1: NO − Isolate Triggers Second E/F 0
*−Change 0−Skip
```

YES The event flag is triggered when the input is isolated.

NO The event flag is not triggered by this condition.

Alarm triggers second event flag

When enabled, the event flag programmed in “Second event flag” on page 76 is triggered when this input is in alarm.

```
1: NO − Alarm Triggers Second E/F 0
*−Change 0−Skip
```

YES The event flag is triggered when the input generates an alarm.

NO The event flag is not triggered by this condition.

Bypass input in Stay Mode

When enabled, the input will not activate when the associated area(s) are in stay mode. The panel can have areas in stay mode via control using CTPlus or the Mobile App.

```
1: NO – Bypass input in Stay Mode
*−Change 0−Skip
```

YES If the areas to which the input is assigned are in stay mode and the input is unsealed, then the input does not generate an alarm.

NO If the areas to which the input is assigned are in stay mode and the input is unsealed, then the input generates an alarm as normal.

Option 2: Area database

Areas determine how the system is partitioned, and therefore provides the ability to limit users to performing functions only in the areas relevant to their role.

A worksheet is provided to record programming details and to further describe this option. See “Area worksheet” on page 252.

Select area to program

Enter an area number in the range 1 to 99, and then press [ENTER].

```
Area Database
Area No:
```

Area name

Program a name to identify the area (for example, to select the area to arm or disarm).

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Exit time

Every area has an exit timer, which can be used for entry/exit input types (3, 4, 13, 14, 41, 42, 61, and 62). The exit timer allows users to arm an area prior to leaving the premises, without generating an alarm. Only after the exit timer expires can an alarm occur.

```
Area 1:>Exit−Time 60 Entry−Time 30
Exit:
```

Enter the required exit time in the range 0 to 255 seconds, and press [ENTER] [ENTER] to save the time and move to the next screen.

If inputs are assigned to more than one area, the longest exit time is used.

Tip: A number displayed after the first colon (for example “Area 1:48”) indicates the number of seconds remaining in the area’s exit timer when the area was disarmed. No number indicates that the area timer expired.

The exit time helps determine how long the exit console warning will last if it is enabled. See “Entry and exit console warning” on page 92 for more information.

Entry time

Every area has an entry timer, which can be used for entry/exit input types (3, 4, 13, 14, 41, 42, 61, and 62). The entry timer allows users to enter the premises prior to disarming, without generating an alarm. A user can disarm the area whilst the entry time is running without generating an alarm.

```
Area 1:> Exit−Time 60 Entry−Time 30
Entry:
```

Enter the required entry time in the range 0 to 255 seconds, and press [ENTER] [ENTER] to save the time and move to the next screen.

If inputs are assigned to more than one area, the longest entry time is used.

The entry time helps determine how long the entry console warning will last if it is enabled. See “Entry and exit console warning” on page 92 for more information.

Area Account

CID reporting account numbers are four digits long, and are used for reporting via Contact ID Modem format and for reporting via IP Receiver format.

```
1: Area Account: 0000
Account:
```

Program area account numbers as follows:

- If the system has account numbers for each area, program the account number for each area on which you want to report alarms.

- If the system has only one account number, program 0000 for each area on which you want to report alarms.

In a communication path that will be used for reporting set "Area account codes" to Yes to enable this path to use the area account code. See “Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Use Area account codes” on page 136.

Siren event flag

The siren event flag is set to 1 by default and does not need to be changed unless you want to have different sirens activated for each area.

This event flag is triggered when an input generates an alarm (if the input’s siren event flag set to YES). Each area can have its own external siren, using different event flags for each area.

```
1: Siren Event Flag 1
Event Flag:
```

Enter the event flag number, and then press [ENTER]. Event flag 1 is selected by default.

If no change is needed, press [ENTER] to go to the next option.

Area accessed event flag

This event flag activates when the area is in access.

```
1: Accessed No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Unsealed event flag

This event flag indicates if any input in the area is unsealed, excluding inputs that can be used to change the status of an area, or used for cameras.

```
1: Unsealed No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Isolate event flag

An input in this area has been isolated.

```
1: Isolate No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Secure alarm event flag

This event flag activates on an alarm when the area is armed.

```
1: Secure Alarm No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Access alarm event flag

This event flag activates on an alarm when the area is disarmed.

```
1: Access Alarm No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Local alarm event flag

This event flag activates on local alarms from, for example, fire door, 24-hour local fail input types, and so on (types 15, 16, 18, 21, 30, 41, 42, 44, and 56) in the area. See “Input types” on page 229.

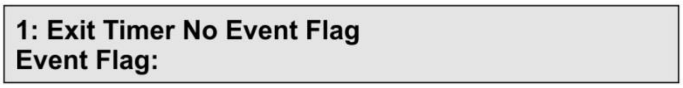
```
1: Local Alarm No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Exit timer event flag

This event flag activates when the exit timer for the area is running.



```
1: Exit Timer No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Note: Enter the same event flag number here as for “Console trigger event flag” on page 186 if you want RAS to beep during the exit timer.

Entry timer event flag

This event flag activates when an entry timer for the area is running.

```
1: Entry Timer No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Note: Enter the same event flag number here as for “Console trigger event flag” on page 186 if you want RAS to beep during the entry timer.

Warning timer event flag

This event flag activates to indicate that a user category is running and the area is about to be armed or that a test mode is in progress and the test is about to end.

```
1: Warning Timer No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Camera event flag

This event flag activates when an input with the appropriate input type and the camera event flag set to YES generates an alarm and the area is disarmed.

```
1: Camera No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

The camera event flag may be reset in the following ways:

- The default behaviour allows anybody to reset the camera event flag (and stop the cameras) from a keypad via [ENTER] [ENTER] 0 [ENTER].
- If the system option “Disable 0 ENTER for Camera Reset” is set to YES, then only an authorised user can reset the camera event flag (and stop the cameras) from a keypad via the user’s PIN.

- An input assigned input type 9 (reset delayed inputs) can be used to stop cameras from operating.

Pre-alarm timer event flag

This event flag indicates that a delayed holdup alarm input is active and the delay timer is running.

```
1: Pre-Alarm Timer No Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

If no event flag is needed, press [ENTER] to go to the next option.

Out-of-hours time zone

Enter a time zone number if you want to report an out of hours access alarm if the area is in access (disarmed) outside of the specified time zone.

```
1: Out Of Hour Tz: 0
Enter Tz:
```

Enter the time zone number, and then press [ENTER].

Area disarm time

User categories can disarm an area for a timed disarm period. An area disarm time greater than 0 will override any user category time for this area.

```
1: Area Disarm Time: 0 Mins
Enter Mins:
```

Enter the minutes, and then press [ENTER].

Perimeter area

This option applies only to “internal” areas that contain inputs programmed as handover input types 4, 14, 61 and 62 where you want the internal area to have a designated perimeter area.

```
1: Has Perimeter Area: 0
Area:
```

Enter the number of the area that contains entry/exit inputs on the perimeter of the premises, and then press [ENTER].

When the entry timer on the perimeter area is activated (for example, by someone opening a door) any internal areas linked by this option are notified. At this point all handover input types in the internal areas will be suppressed for the perimeter area’s entry time.

If the internal area is disarmed while the perimeter area is still entry timing, then the perimeter area will cancel the entry timer and start the exit timer: this allows the perimeter to remain armed while the internal area is occupied.

Arming the internal area when the perimeter area is armed will re-activate the exit timer on the perimeter area to allow people to exit the building without activating an alarm on the perimeter area.

When the perimeter area is disarmed, the internal area’s handover inputs behave like entry/exit inputs.

The internal area and the perimeter area can be armed and disarmed independently from each other. However, when the internal area is secure (armed), the behaviour of the internal area’s handover inputs depends on whether the perimeter area is armed or disarmed:

- If the perimeter area is armed (secure), then the perimeter area’s entry or exit timers apply to the internal area.
- If the perimeter is disarmed (in access), then the internal area’s entry or exit timers apply to the internal area.

Note: The perimeter area must have longer entry and exit times than any of the internal areas.

Option 3: RAS database

Remote arming stations (RASs) are devices used to provide alarm system control (such as arming or disarming), to provide access control (such as unlocking a door), and for programming the system.

Alarm groups control what functionality and menu access is available at a RAS, in a similar manner to a user’s alarm group controlling what functionality and menu access is available to the user. When a user enters their PIN at an arming station, that user will be able to perform functions (such as alarm control) and see menus (for example, to program users) that are available to both the RAS and the user via their respective alarm groups.

With RASs, you have the option to program two different alarm groups:

- See “RAS model

Select the RAS model attached to the ChallengerPlus panel. This will allow certain options in the panel to be configured to ensure optimal communications.

```
1:RAS Model is:
Model No:
```

The model may be selected from a pre-defined list, as detailed in Table 8.

Table 8: RAS models summary

Model No	RAS model	LCD	Keypad	Card Reader	Mag Swipe	LEDs
1	TS0003		Yes			4
2	TS0004	Yes	Yes			16
3	TS0006		Yes			4
4	TS0007		Yes		Yes	4
5	TS0008		Yes		Yes	4
6	TS0801	Yes	Yes			8
7	TS0804	Yes	Yes			16
8	TS0862			Yes		2
9	CA1110	Yes	Yes			16
10	CA1111	Yes	Yes			16
11	CA1115	Yes	Yes	Yes		16
12	CA1116	Yes	Yes	Yes		16
13	TS0870			Yes		2
14	TS0870H			Yes		2
15	TS0870D			Yes		2
16	TS1001	Yes	Yes			8
	TS1162		Yes			3

Area alarm group” on page 86.

- See “Menu alarm group” on page 87.

A worksheet is provided to record programming details and to further describe this option. See “RAS worksheet” on page 254.

Poll RAS

In order to be used, a RAS number has to be polled. Polling enables communication between the RAS and the control panel. Challenger automatically uses data encryption when connecting to devices that support encryption.

```
1.2,3:65!
Poll RAS:
```

Enter the RAS number to be polled, and then press [ENTER]. Repeat for all RAS numbers to be polled.

Notes:

- RASs on LAN 1 or LAN 2 can be configured with addresses in the range 1 to 16. The first RAS on LAN 1 is configured as RAS 1, and is polled as RAS 1. The first RAS on LAN 2 is configured as RAS 1, but must be polled as RAS 65.

- Only polled RASs can be retrieved from the panel (such as by retrieving to management software or backing up to SD card).

To deactivate a RAS number that is already polled, enter the RAS number again, and then press [ENTER].

Press [ENTER] again to move to the next option.

The display shows the RASs currently being polled, with each RAS number followed by a symbol to indicate whether:

- the RAS is responding to polling
- data encryption is supported

Refer to Table 7 below for an explanation of the polling symbols.

Table 7: RAS polling indications

Symbol	Application
.	The RAS is online (responding to polling), encryption present
!	The RAS is offline, encryption present
,	The RAS is online (responding to polling), encryption not present
:	The RAS is offline, encryption not present

Notes:

- An offline RAS number initially displays “!” or “:” (as appropriate) whilst communication is established. Press the * key to update the display to indicate the polled state.
- If you need to replace a RAS, we recommend that you de-poll the old RAS before removing it. Install the new RAS according to its installation instructions. Some RAS models will not go online otherwise.

Select RAS to program

Enter the RAS number in the range 1 to 16 and 65 to 80 to be programmed, and then press [ENTER].

Arming Station Details
RAS No:

RAS name

Program a name to identify the RAS (for example, to identify its location and type).

1:
(1)−Edit

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Note: The RAS name is the same as the (same numbered) door name, programmed in “Option 40: Door/lift names and E/F trigger” on page 199.

RAS model

Select the RAS model attached to the ChallengerPlus panel. This will allow certain options in the panel to be configured to ensure optimal communications.

```
1:RAS Model is:
Model No:
```

The model may be selected from a pre-defined list, as detailed in Table 8.

Table 8: RAS models summary

Model No	RAS model	LCD	Keypad	Card Reader	Mag Swipe	LED
1	TS0003		Yes			4
2	TS0004	Yes	Yes			16
3	TS0006		Yes			4
4	TS0007		Yes		Yes	4
5	TS0008		Yes		Yes	4
6	TS0801	Yes	Yes			8
7	TS0804	Yes	Yes			16
8	TS0862			Yes		2
9	CA1110	Yes	Yes			16
10	CA1111	Yes	Yes			16
11	CA1115	Yes	Yes	Yes		16
12	CA1116	Yes	Yes	Yes		16
13	TS0870			Yes		2
14	TS0870H			Yes		2
15	TS0870D			Yes		2
16	TS1001	Yes	Yes			8
	TS1162		Yes			3

Area alarm group

An area alarm group defines the alarm control functionality that any user can perform at the RAS, subject to the functionality that the user's alarm group provides.

For example, to arm area 1, both the RAS and the user must have alarm system control for area 1. All alarm control options will be taken from the area alarm group programming.

```
1: Alm−Grp: 2−Master RAS or Door
Alm−Grp:
```

Enter the area alarm group number, and then press [ENTER]. See "Option 5: Alarm groups" on page 96 for details.

Menu alarm group

A menu alarm group defines which menus that a user can access on the RAS's LCD screen, subject to the menus that the user's alarm group provides. For example, to access the Install menu, both the RAS and the user must be permitted to see to the Install menu.

The menu alarm group provides the menus that can be accessed from this RAS regardless of what menus are available in the area alarm group. The alarm group nominated here does not contribute any alarm control functionality to the RAS.

Guidelines for using the menu alarm group:

- The user’s alarm group and the RAS’s menu alarm group must share at least one area for the user to see any menus on the RAS’s LCD screen.
- If different alarm groups are used for the area alarm group and the menu alarm group, then both alarm groups must have the same settings for “alarm system control”, “prompt with list of areas”, and “keypad duress”.
- If two different alarm groups are not needed, then you can assign the same alarm group number to both the area alarm group and the menu alarm group. Alternatively, program the menu alarm group as alarm group 1 (no access) in order to use the area alarm group for both.

```
1: Alm−Grp: 2−Master RAS or Door
Menu Alm−Grp:
```

Enter the menu alarm group number, and then press [ENTER]. See “Option 5: Alarm groups” on page 96 for details.

Door event flag

If the RAS is used to unlock a door, assign a door event flag to the RAS. The door event flag will be activated (for the doors unlock time programmed in “Option 6: Timers” on page 104) when a valid code is entered at the RAS or a valid card is badged.

```
1: Has No Door Event Flag
Event Flag:
```

Enter the event flag number, and then press [ENTER].

Relay number

The RAS’s output can have any relay number assigned to it.

```
1: Output Has No Relay Assigned
Relay No:
```

Enter a relay number in the range 1 to 512 that will drive the relay or output on this arming station, and then press [ENTER].

Note: Use a value of 0 for TS0004 and TS0210 RASs.

RAS programming options

Program the RAS according to its characteristics (for example, if the RAS has an LCD, set the LCD Arming Station option to YES). Refer to Table 8 on page 87 or the specific RAS's installation guide for details. See also "Using card readers for alarm control" on page 38.

Details of the RAS programming options follow.

LCD arming station

Applies to RAS models with LCD or touch screen, see Table 8 on page 87.

```
1: NO − LCD Arming Station
*−Change 0−Skip
```

YES This RAS is an LCD arming station.

NO This RAS does not have an LCD screen or a touch screen.

Toggle keyboard control

Applies to RAS models with keypad or touch screen, see Table 8 on page 87.

```
1: NO − Toggle Keyboard Control
*−Change 0−Skip
```

YES The [ON] and [OFF] keys lose their function. For arm control the user must enter the user code followed by [ON], [OFF], or [ENTER]. If a list of areas appears, pressing the area number and [ENTER] toggles the status of the area. If no list appears, the status of the areas is toggled immediately.

NO Normal alarm control.

ENTER key opens door only

Applies to RAS models with keypad or touch screen, see Table 8 on page 87. Set this option to YES for the best user interface on LCD RASs.

```
1: NO − ENTER Key Opens Door Only
*−Change 0−Skip
```

YES The [ENTER] key unlocks the door but the [ON] and [OFF] keys are used for alarm control. When set to YES, keypad duress functionality requires the use of the [ON], [OFF] or [*] keys — but not the [ENTER] key.

NO The [ENTER] key unlocks the door and also provides alarm control and resets alarms.

Door event flag on alarm codes

Door codes must be at least four digits long and are determined by the setting of the alarm prefix length. See "Number of prefix " on page 112.

```
1: NO − Door Event Flag On Alarm Codes
*−Change 0−Skip
```

YES The door event flag will operate (unlock the door) for either a valid alarm code or a valid door code.

NO The door event flag will operate (unlock the door) only for a valid door code.

Display shunting on LCD

Applies to RAS models with LCD or touch screen, see Table 8 on page 87.

```
1: NO − Display Shunting on LCD
*−Change 0−Skip
```

YES When an input is shunted, the text ‘Input Shunted’ will appear on the display (LCD RAS only).

NO Nothing is shown when an input is shunted.

Disarm/arm using one key

Applies to RAS models with keypad, see Table 8 on page 87.

```
1: YES − Disarm/Arm Using One Key
*−Change 0−Skip
```

YES After entering the user code, arm or disarm areas by entering the (single-digit) number of the area without pressing [ENTER]. Areas 10 to 99 cannot be controlled from this keypad when this option is set.

NO Normal alarm control.

Note: This option is not compatible with TS1001 Touch Screen RAS. Do not use.

Cards auto disarm

Applies to RAS models with card reader, see Table 8 on page 87.

```
1: NO − Cards Auto Disarm
*−Change 0−Skip
```

YES The areas assigned to the user and the RAS in their alarm groups will automatically disarm when the card is presented to access.

NO The card only activates the door function unless Card Always Disarms/Arms is set to Yes, or ON/OFF buttons (TS0064 Expanded Button Interface) are used.

Cards always disarm/arms

Applies to RAS models with card reader, see Table 8 on page 87. The card user’s alarm group and the RAS’s (reader’s) alarm group must both allow arm and/or disarm functions before a card can be used to arm and disarm.

```
1: NO − Cards Always Disarm/Arm
*−Change 0−Skip
```

YES The areas assigned to the user and the RAS in their alarm groups will automatically disarm or arm when the card is presented. Toggle Keyboard Control must be set to YES.

NO The card only activates the door function unless Card Auto Disarms is set to Yes, or ON/OFF buttons (TS0064 Expanded Button Interface) are used.

Reset from RAS without code

Note: Applies to RAS models with LCD and keypad, or touch screen, see Table 8 on page 87.

```
1: NO − Reset From RAS Without Code
*−Change 0−Skip
```

YES Reset alarms by pressing [ENTER] [ENTER] (show alarms) followed by 0 [ENTER]. The areas in alarm must be assigned to the RAS alarm group.

NO An authorised user code is required to reset alarms.

Restricted user category to disarm

```
1: NO − Restricted User Category To Disarm
*−Change 0−Skip
```

YES Users with user categories cannot manually arm.

NO There is no restriction.

Cards arm after three badges

Applies to RAS models with card reader, see Table 8 on page 87.

```
1: NO − Cards Arm After 3 Badges
*−Change 0−Skip
```

YES The assigned areas will arm with three badges of a valid card within 10 seconds (if “Cards auto disarm” on page 90 is set to YES).

NO Normal alarm control.

Card and code

Applies to RAS models with card reader, see Table 8 on page 87.

```
1: NO − Card & Code
*−Change 0−Skip
```

YES Both card and PIN are required for access to RAS functions. After the card is presented, the PIN must be entered before the RAS Card and PIN time expires. Card to code time is programmed in timers.

NO PIN alone is required for access to RAS functions.

Entry and exit console warning

The RAS can have an audible and visible console warning during entry and exit times.

During the RAS’s entry time period the keypad buzzer will beep and the RAS will display:

```
Entry,
```

For the last 10 seconds of the entry time period, the keypad buzzer will sound a constant tone and the RAS will display:

```
Entry Ending,
```

Similarly, during the RAS’s exit time period the keypad buzzer will beep and the RAS will display:

```
Exit,
```

For the last 10 seconds of the exit time period, the keypad buzzer will sound a constant tone and the RAS will display:

```
Exit Ending,
```

The entry time period for the RAS is determined by the maximum of the entry time settings for all associated areas. See “Entry time” on page 78. Similarly, the exit time period for the RAS is determined by the maximum of the exit time settings for all associated areas. See “Exit time” on page 78.

```
1: NO − Entry & Exit Console Warning
*−Change 0−Skip
```

YES Enable the entry and exit console warnings.

NO Disable the entry and exit console warnings.

Note: Entry and exit console messages are not displayed during alarms.

Area LED assignment

By default, the RAS’s areas LEDs are mapped to areas 1 to 16.

```
1: Area for LED 1 is 1.
Area, 0−Skip
```

If you want to assign a different area number to the displayed area LED, press a number in the range 1 to 99, and then press [ENTER] to move to the next area LED. If you want to disable an area LED, press *, and then press [ENTER] to move to the next area LED.

Alternatively, press [0] to exit.

Option 4: DGP database

Data gathering panels DGP are devices used to send information to the control panel and to provide added access control functionality.

A worksheet is provided to record programming details and to further describe this option. See “DGPs worksheet” on page 256.

Poll DGP

Each DGP must be polled to enable communication between the DGP and the control panel. The display shows the DGPs currently polled. Challenger automatically uses data encryption when connecting to devices that support encryption.

```
1.2,3:4!
Poll DGP:
```

Enter the DGP number to be polled, and then press [ENTER]. Repeat for all DGP numbers to be polled.

Notes:

- DGPs on LAN 1 can be configured with addresses in the range 1 to 15, and DGPs on LAN 2 can be configured with addresses in the range 1 to 16. The first DPG on LAN 1 is configured as DGP 1, and is polled as DGP 1. The first DGP on LAN 2 is configured as DGP 1, but must be polled as DGP 17. Refer to Table 25 on page 225 for details of addressing and polling.
- Only polled DGPs can be retrieved from the panel (such as by retrieving to management software or backing up to SD card).

To deactivate a DGP number that is already polled, enter the DGP number again, and then press [ENTER].

Press [ENTER] again to move to the next option.

The display shows the DGPs currently being polled, with each DGP number followed by a symbol to indicate whether:

- the DGP is responding to polling
- data encryption is supported

Refer to Table 9 on page 94 for an explanation of the polling symbols.

Table 9: DGP polling indications

Symbol	Application
.	The DGP is online (responding to polling), encryption present
!	The DGP is offline, encryption present
,	The DGP is online (responding to polling), encryption not present
:	The DGP is offline, encryption not present

Tip: An offline DGP number initially displays “!” or “:” (as appropriate) whilst communication is established. Press the * key to update the display to indicate the polled state.

Note: Intelligent Access Controllers may be addressed in the range 1 to 12 on LAN 1 and 17 to 28 on LAN 2.

Deactivating a DGP address number clears all alarms for inputs and system points for that DGP address. If the next DGP address number is not polled, alarms on any of the 32 inputs that belong to the DGP are cleared.

Press [ENTER] again to program the DGP details.

DGP details

Enter the DGP’s address in the range 1 to 15 on LAN 1 and 17 to 32 on LAN 2, and then press [ENTER].

```
DGP Details
DGP No:
```

DGP Name

Program a name to identify the DGP (for example, to identify its location and type).

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

DGP Model

Select the DGP model attached to the ChallengerPlus panel. This will allow certain options in the panel to be configured to ensure optimal communications.

```
1:DGP Model is:
Model No:
```

The model may be selected from a pre-defined list, as detailed in

Table 10.

Table 10: DGP types

Model No	Mode No	Model number	Description
0		TS0820	Challenger V8 DGP
1		TS0867	V8 Four Door Controller
2		TS0869	V8 Four Lift Controller
3		TS1020	Challenger10 DGP
4		TS0866	V8 Four Door Controller (Non-Wiegand)
5		TS0825	Inovonics FA Wireless DGP
6		TS0825E	Inovonics EchoStream Wireless DGP
7		TS1066	Network Access Controller *Note: When this Model is selected, a Mode number must also be set*
-	0	TS1066	None (IP Direct mode)
-	1	TS1066	Classic
-	2	TS1066	IP Extended
-	4	TS1066	Classic with 8 doors
-	5	TS1066	IP Extended with 8 doors
8		TS1061	Dual Wiegand Interface

Option 5: Alarm groups

Alarm groups enable users, inputs, and RASs to control the system’s alarm functions (also called alarm control).

An alarm group’s functionality is controlled by the following:

- **Areas**—determines the areas you want this alarm group to control.
- **Time zone**—determines the time zone applicable to this alarm group. Functions assigned via this alarm group will be applicable only for the periods allowed by the time zone (or when the soft time zone is valid). Also, both a user’s alarm group time zone and the RAS’s (or door’s) alarm group time zone have to be valid.
- **Menus**—determines access to the Challenger User menus that the user will have for this alarm group (see Table 2 on page 14).
- **Options**—determines access to system functions that the user or RAS will have for this alarm group. If you do not select User Alarm Group, then you will not be able to assign the alarm group to any user.
- **Alternate alarm group**—used whenever the original alarm group is disabled due to an invalid time zone.

Alarm groups can be assigned to:

- Users
- RASs 1 to 16 and 65 to 80

- Doors 17 to 64 and 81 to 128
- Area control input types 6, 31, 34 and 35
- Auto reset functionality
- Arm or disarm via time zone functionality

Alarm groups provide enormous flexibility when determining a user’s access to, and control of, the system.

Note: You must be extremely careful when changing alarm groups. Both the functions performed by user in the alarm group and the functions available at RASs with that alarm group will be affected.

A function that is provided to users via their alarm group is only valid when:

- Program settings in other sections of the same alarm group allow it. Example: Restricting alarm system control to Reset Only would be invalid unless the alarm group has been allowed alarm system control. If Reset Only is set to YES, Alarm System Control must be set to YES.
- The user’s alarm group has the same program setting as the alarm group of the RAS or door the user is using. Example: If the Prompt with List of Areas is set to YES in the user’s alarm group, it must also be set to YES in the alarm group of the RAS or door. If it is not, areas are not listed when arming/disarming.
- The user’s alarm group includes the areas assigned to the alarm group of the RAS or door the user is using. Example: If a user’s alarm group has areas 1, 2, and 3 and the alarm group of the RAS or door has areas 2 and 3, only the functions for areas 2 and 3 are valid.

Alarm group application

Alarm groups may be fixed or have programmable options, as listed in “Alarm group default settings” on page 239. Alarm groups are used as follows:

- Alarm Group 1 “No Access”
- Alarm Group 2 “Master RAS or Door” contains Area Group 1 and the default settings for the master RAS (RAS 1 on LAN 1).
- Alarm Group 3 “Master Code” is fixed. It contains Area Group 1 and the default settings for the master user 50 (Installer).
- Alarm groups 4 to 10 are spare. Do not use.
- Alarm Group 11–High Level User Master contains Area Group 1 and all User menus except 19–Install.
- Alarm Group 12–Low Level User Master contains Area Group 1 and User menus 1, 5, 9, 10, 11, 14, 15, and 16.
- Alarm Group 13–All Area User Code contains Area Group 1 and User menus 1, 5, 9, 10, and 11.

- Alarm Groups 14 to 29 are intended for RASs that control a single area and User menus 1, 5, 9, 10, and 11.
- Alarm Groups 30 to 255 have no default programming and are intended to be programmed for users or RASs according to the system requirements.

Programming alarm groups

A worksheet is provided to record programming details and to further describe this option. See “Alarm group worksheet” on page 257.

Alarm group number

Every alarm group has a number in the range 1 to 255.

```
Alarm Groups **WARNING**
Alm−Grp:
```

Enter the alarm group number, and then press [ENTER].

Alarm group name

Program a name to identify the alarm group, or use the default name (if applicable).

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Areas assigned

An alarm group can only control the functions of areas that are assigned to it.

An alarm group can be linked to a single area or to an area group:

- When linked to an area, the alarm group controls the area's permissions for arming, disarming, alarm reset, and for timing.
- When linked to an area group, the area group controls each area's permissions for arming, disarming, alarm reset, and for timing.

```
Alarm Grp:30 Area 0
'*'−Grp, Area:
```

To link a single area to the alarm group, enter the area number to be controlled by the alarm group, and then press [ENTER].

Alternatively, press [*] to link an area group to the alarm group.

```
Alarm Grp:30 Area Group 0
'*'−Grp, Grp:
```

Enter the area group number to be controlled by the alarm group, and then press [ENTER].

To remove a programmed area or area group, press [0] [ENTER] when prompted for the area or area group number.

User alarm group

When programming a new user record in User menu option 14. Program Users, a list of designated “user alarm groups” are displayed on the RAS for assigning to the new user. The list of designated “user alarm groups” depends on the alarm group (and alternate alarm group, if applicable) of the person doing the programming. You cannot assign an alarm group to a new user that has more permissions than you have.

```
NO − Can This GRP Be Assigned to Users
*−Change 0−Skip
```

YES This alarm group can be assigned to users.

NO This alarm group is only assigned to an input, door, RAS, auto reset, or arm/disarm via time zone.

0 Press 0 on this or subsequent screens to skip straight to “User menu options” on page 103.

Alarm system control

```
NO − Alarm System Control
*−Change 0−Skip
```

YES A user or RAS with this alarm group can arm or disarm the areas in the alarm group. This option must be set to YES if any of the user categories in the alarm group are set to YES.

NO Do not enable alarm system control. Access control functions and user menu options specified are still valid.

Prompt with list of areas

```
NO − Prompt With List of Areas
*−Change 0−Skip
```

YES After the user has entered a PIN and pressed [ON] or [OFF], the areas assigned to the user are displayed. The user can then select from the arm/disarm options.

NO The areas assigned to the user are not displayed. Areas are immediately armed/disarmed once the user has entered a PIN and pressed [ON] or [OFF].

Keypad duress

```
NO − Can Users Activate Keypad Duress
*−Change 0−Skip
```

YES A user with this alarm group can enter a duress code on a keypad to activate a duress alarm.

NO Keypad duress cannot be activated. A duress code is treated as an invalid code.

See also “Using keypad duress” on page 54.

Reset system alarms

```
NO − Reset System Alarms
*−Change 0−Skip
```

YES A user with this alarm group can reset the latching system alarms. The user’s alarm group must allow arming, disarming, and resetting; and “System alarms” on page 117 must also be set to YES.

NO A user cannot reset latching system alarms.

Can area be armed

```
NO − Can Area be Armed
*−Change 0−Skip
```

Note: This option applies only when the alarm group is linked to a single area. Skip this option if linked to an area group.

YES A user with this alarm group can arm the area.

NO A user with this alarm group cannot arm the area.

Can area be disarmed

```
NO − Can Area be Disarmed
*−Change 0−Skip
```

Note: This option applies only when the alarm group is linked to a single area. Skip this option if linked to an area group.

YES A user with this alarm group can disarm the area.

NO A user with this alarm group cannot disarm the area.

Can area be reset

```
NO − Can Area be Reset
*−Change 0−Skip
```

Note: This option applies only when the alarm group is linked to a single area. Skip this option if linked to an area group.

YES A user with this alarm group can reset alarms for the area.

NO A user with this alarm group cannot reset alarms for the area.

Can area be timed

An area can be timed via a user category to allow a user to disarm the area for a timed interval (in which case disarming must be permitted), or to allow the area to be automatically armed via vault programming (in which case arming must be permitted).

```
NO − Can Area be Timed
*−Change 0−Skip
```

Note: This option applies only when the alarm group is linked to a single area. Skip this option if linked to an area group.

YES Depending on the application, a user with this alarm group can disarm the area for the user category time, or automatically arm another area (via vault programming).

NO A user with this alarm group cannot use timed disarming or arming functionality.

Disable auto-deisolate

Select this option to prevent certain users (for example, cleaners) from being able to automatically deisolate inputs in the area they disarm.

```
NO − Disable Auto-Deisolate
*−Change 0−Skip
```

YES A user with this alarm group can disarm areas with isolated inputs remaining isolated even if the system is programmed to automatically deisolate (sealed) isolated inputs.

NO Disarming the area will automatically deisolate sealed and isolated inputs in the area, if the system is programmed to automatically deisolate inputs.

See also “Automatic deisolate” on page 116.

Auto isolate unsealed inputs

```
NO − Auto Isolate Unsealed Inputs
*−Change 0−Skip
```

YES When the arming starts, all unsealed inputs are automatically isolated and the system is armed without causing an alarm. Alarm system control must also be set to YES.

NO The system cannot be armed if there are unsealed inputs, unless “Forced arming when inputs unsealed” below is set to YES.

Forced arming when inputs unsealed

NO − Forced Arming When Inputs Unsealed
***−Change 0−Skip**

YES The check for unsealed inputs is ignored. If there are unsealed inputs when the arming procedure is started, the system still arms (the unsealed inputs might cause an alarm).

NO The system cannot be armed if there are unsealed inputs, unless “Auto isolate unsealed inputs” on page 101 is set to YES.

Note: See “Enable exit fault reporting” on page 120 if you want to report alarms from non-entry/exit type inputs as “exit error alarms”.

Prevent forced disarming

This setting controls the treatment of unsealed inputs during the disarming procedure and may be used if there are access alarm input types such as type 1 or type 11 in the system.

NO − Prevent Forced Disarming
***−Change 0−Skip**

YES The area cannot be disarmed if there are unsealed inputs.

NO The area can be disarmed even if there are unsealed inputs.

Can user access via remote

NO − Can User Access Via Remote
***−Change 0−Skip**

Note: This option is not currently supported. Do not use.

User categories (1 through 8)

User categories assigned to an alarm group provide timing functionality via a corresponding user category time (see “Option 15: User category” on page 163 and “User category time” on page 104).

If multiple user categories are assigned to an alarm group, then the lowest user category number applies. System functionality can depend on the alarm group assigned to a user, and the alarm group assigned to a RAS. In these cases, the lowest common user category number applies.

For example, if a user has an alarm group containing user categories 3 and 4, and a RAS has an alarm group containing user categories 1, 2, 3, and 4, then only user category 3 would apply to that user at that RAS.

When set to YES, the user category activates when a user with this alarm group enters their PIN (or badges their card).

```
NO − Link User to Category 1
*−Change 0−Skip
```

YES Activates the displayed user category.

NO The displayed user category is not activated.

No arming if user category not timing

This option prevents the area from being automatically rearmed without a user category. For example, a guard might have a user category that automatically re-arms an area when the user category timer expires. However, if someone else disarmed the area (the user category timer isn’t running), then the guard’s user category will not automatically re-arm the area.

```
NO − No Arming If User Cat Not Timing
*−Change 0−Skip
```

YES Prevents automatic re-arming when an area is occupied by non-user category staff.

NO Normal user category programming applies.

Enable area search

```
NO − Enable Area Search
*−Change 0−Skip
```

When enabled, a user with this alarm group must perform an area search as part of the disarming process during the “Area Search TZ” specified in System Options). See “Using Area Search” on page 56 for details.

User menu options

These settings determine which user menu options are available in this alarm group to users or RAS. Each user menu is displayed and must be set to YES for it to be available to the alarm group.

```
NO − 1−Panel Status
*−Change 0−Skip
```

Refer to Table 2 on page 14 for a list of user menu options.

Alarm group time zone

Specify a time zone to apply to this alarm group. The alarm group is only available if the time zone is valid (see “Option 13: Time zones” on page 161 and “Option 22: Soft time zones” on page 175).

```
Alm−Grp 30 No Time Zone
Time Zone:
```

Enter the time zone number for this alarm group, and then press [ENTER].

Alternate alarm group

You can program each alarm group to have an alternate (alternative) alarm group. The alternate alarm group is used whenever the original alarm group is disabled due to an invalid time zone. The alternate alarm group can have different areas or options than the original alarm group.

For example, during normal working hours, users can arm and disarm from a list. After hours, only arm/alarm reset is allowed without presenting a list of areas.

The alternate alarm group can also be programmed with an alternate alarm group and so on, up to three alarm groups (the original plus two alternates). If a function is denied by the time zone of one alarm group, the next will be checked, and so on.

```
Grp 30 Alt−Grp 1 − No Access
Alm−Grp:
```

Enter the alternate alarm group number for this alarm group, and then press [ENTER].

Option 6: Timers

Timers are accurate on ± 1 of the value entered, so a timer set for 20 seconds will end somewhere between 19 and 21 seconds. Therefore, avoid using values of 1 second or 1 minute.

A worksheet is provided to record programming details and to further describe this option. See “Timers worksheet” on page 258.

User category time

Program times (2 to 255 minutes) for user categories 1 through 8 for the time that the user category timer is to run.

Notes:

- If set to “0”, the areas will not arm automatically.

- The user category time will be overridden by the area disarmed time (if programmed) in the area database.

```
User Category 1 Set to (Min). 0
Time:
```

Enter the time in minutes for user category 1, and then press [ENTER].

Repeat for user categories 2 through 8.

Access test time

```
Access Test Set To (Min). 15
Time:
```

Enter the time to perform the access test (2 to 255 minutes), and then press [ENTER].

Secure test time

```
Secure Test Set To (Min). 15
Time:
```

Enter the time to perform the secure test (2 to 255 minutes), and then press [ENTER].

Warning time

When user categories are used and areas are timed, a warning will sound (if a warning time is programmed) indicating the areas are about to arm.

```
Warning Time Is Set To (Min). 5
Time:
```

Enter the time this warning will sound (2 to 255 minutes), and then press [ENTER].

The warning time must always be set for a shorter time than any user category disarmed time. The warning time must always be shorter than the shortest user category time and should be at least 2 minutes.

Delay holdup time

Delay holdup time is the interval before an alarm from a delayed input type (for example, a holdup alarm) is reported to the remote monitoring company (the delay time is ignored if another delayed input type has already been activated).

```
Delay Holdup Time Set To (Sec). 60
Time:
```

Enter the delay time (2 to 255 seconds), and then press [ENTER].

Suspicion time

Suspicion time is the interval that a camera continues to operate after a suspicion input type (7, 40, or 47) has switched to sealed state.

```
Suspicion Time Is Set To (Sec). 15
Time:
```

Enter the time (2 to 255 seconds), and then press [ENTER].

Service time

User menu 17 can be used to give access to service technicians. The alarm group for the technician needs time zone 25 to be assigned. When a user enables the service technician, time zone 25 will be valid during the service time.

```
Service Time Is Set To (Min). 30
Time:
```

Enter the service time (2 to 255 minutes), and then press [ENTER].

Local alarm reminder time

Local alarm reminder time is the interval that can elapse between acknowledging a local alarm and a re-alarm occurring, including the audible alert.

```
Local Alarm Reminder Time (Min). 0
Time:
```

Enter the time (2 to 255 minutes), and then press [ENTER].

Individual input test time

Individual input test time is the interval to perform a test on an individual input, using User menu 12, Test Input.

```
Individual Testmode Time (Min). 5
Time:
```

Enter the maximum time (2 to 255 minutes), and then press [ENTER].

Door(s) unlock time

Door(s) unlock time is the interval that doors will unlock (using the door event flag) to allow doors to be opened. This time value is common for all door event flags from RASs connected to the control panel (doors 1 to 16 and 65 to 80). Doors 17 to 64 and 81 to 128 are connected to DGPs and are individually programmed via the DGP.

```
Door(s) Unlock Time (Sec). 5
Time:
```

Enter the time (2 to 255 seconds), and then press [ENTER].

Tester event flag time

Tester event flag time is the interval that the tester event flag is triggered to activate devices in order to perform a secure test.

Tester Event Flag Time (Sec). 15
Time:

Enter the time (2 to 255 seconds), and then press [ENTER].

Note: 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 sealed state. The event flag used is preset to 16.

Siren time set to

Siren time is the interval that the onboard internal siren drivers activate.

Siren Time Set To (Min). 8
Time:

Enter the time (2 to 255 minutes), and then press [ENTER].

Mains fail time

Mains fail time is the interval before a mains fail is reported to the remote monitoring company.

Mains Fail Time (Min). 0
Time:

Enter the delay time (2 to 255 minutes), and then press [ENTER]. Enter a value of “0” for no delay.

Card to code time

On RASs where card and code are required, the card to code time is the delay between badging the card and entering the PIN.

Card to Code Time (Sec). 8
Time:

Enter the delay time (2 to 255 seconds), and then press [ENTER].

Minimum area search time

Min Area Search Time (Min). 0
Time:

Enter the smallest amount of time (2 to 255 minutes) in which an area search may be completed, and then press [ENTER]. See “Using Area Search” on page 56 for details.

Maximum area search time

Max Area Search Time (Min). 142
Time:

Enter the largest amount of time (2 to 255 minutes) in which an area search may be completed, and then press [ENTER]. See “Using Area Search” on page 56 for details.

Maximum twin trip time

Max Twin Trip Time (Sec). 0
Time:

Enter the maximum amount of time (1 to 255 seconds) that a twin trip timer may run, and then press [ENTER].

See “Programming twin trip inputs” on page 65 for details.

Option 7: System options

A worksheet is provided to record programming details and to further describe this option. See “System options worksheet” on page 259.

In the CTPlus software the commands below are organised into tabbed panels:

- System Options Part 1
- System Options Part 2, and
- System Options Part 3.

System options part 1

Challenger Number

The Challenger Number associates a Panel with a specific record of data. This field requires a number to be input to associate the Panel with the setting of the System information.

Total disarm

Use this option to program an area (or an area group) to have overriding control over the alarm functionality for designated inputs in another area.

This functionality is particularly useful for disabling alarm inputs that are 24-hour alarm types, where an unsealed input would normally generate an alarm regardless of whether the input's assigned area is armed or disarmed. In this case, the input would be assigned both area 1 (normal area) and area 16 (total disarm area).

When the "total disarm" area (or area group) is:

- Armed, then the input would function as programmed (that is, the input would react according to its type and the other area's armed or disarmed state, as applicable).
- Disarmed, then the input could not go into alarm (except to indicate input tamper).

This functionality can be used for all alarm input types:

- Access alarms—Input types 1 and 11 can generate an alarm when one or more of the areas assigned are in access (disarmed).
- Secure alarms – Input types 2, 3, 4, 13, 14, 28, 60, 61, and 62 can generate an alarm when all of the areas assigned are in secure (armed).
- 24-hour alarms—Input types 5, 29, 33, and 59 can generate the same alarm regardless of area status.
- Access/secure alarms—Input types 8, 15, 21, 22, 30, 40, 41, 42, 44, 45, 46, 47, and 56 can generate different types of alarms when in access and secure (disarmed and armed).

Note: Input tampers will still cause alarms if tamper monitoring is enabled.

Example: Input 6 is a sensor in a vault. It is programmed as input type 5 (24-hour) and is assigned areas 1 and 16. Area 16 is programmed for total disarm. When servicing the vault, area 16 is disarmed, and the effect is that input 6 is disabled until area 16 is armed again.

```
Total Disarm Area 0
'*'−Grp, Area:
```

Enter an area number in the range 1 to 99 to assign an area, and then press [ENTER].

Alternatively, press [*] to assign an area group.

```
Total Disarm Area Group 0
'*'−Chg, Grp:
```

Enter an area group number in the range 1 to 255 to assign an area group, and then press [ENTER].

Press [ENTER] when you are finished adding a total disarm area or an area group.

To remove a programmed area or area group, press [0] [ENTER] when prompted for the area or area group number.

Film low

Film low level is the camera count value for input types 23 to 26 and 36 to 39 at which a film low report is sent to the remote monitoring company.

Film Low is Set to 0800
Film Level:

Enter the film low frame count number, and then press [ENTER].

Film out

Film out level is the camera count value for input types 23 to 26 and 36 to 39 at which an out-of-film report is sent to the remote monitoring company.

Film Out is Set to 1100
Film Level:

Enter the film out frame count number, and then press [ENTER].

Test mode

The test mode setting defines whether a secure test or an access test (input testing interval) starts automatically upon arming or disarming areas that contain the input. Testing of inputs involves monitoring the state of the input whilst changing its state from sealed to unsealed, and then back to the sealed state. This is typically done by, for example, opening and closing a door and then checking the LCD screen to verify that the change was correctly reported. Refer to Testing Input Devices in *ChallengerPlus Administrator’s Manual* for details.

Regardless of the programmed test mode, inputs may also be tested via:

- User menu 12 Test Input
- User menu 13 Start Auto Access Test
- Normal operation over a number of days (see “Test input within no. of days” on page 75).

See also the chapter “Test option” on page 72 for related programming.

0, No Test
Option:

Enter the number for the test mode (see Table 11 below), and then press [ENTER].

Table 11: Test modes

Number	Option	Function
0	No Test	Input testing intervals are not started automatically upon arming or disarming.
1	Enable Auto Test	The access test starts automatically when the system is disarmed. The secure test starts automatically when the system is armed.

2	Manual Access Test/Auto Secure Test	The secure test starts automatically when the system is armed.
3	Auto Access Test Only	The access test starts automatically when the system is disarmed.

For the auto access test to operate, at least one area must be programmed as a vault area. If the system contains a vault area, then the access test operates as follows:

- Disarming the vault area only, starts the access test on the vault area only.
- Disarming all areas (including the vault area), starts the access test on all areas.
- Disarming the non-vault areas only, does not start the access test.

No. of Relay controllers

The value in this record indicates the number of (8-way) relay controllers that are fitted to the main control panel (do not enter values for relay controllers fitted to DGPs). The range of values begins at 0 to indicate either no relay controller or one TS0840 4-Way Relay Card fitted to the control panel (if a TS0840 is fitted, no other relay controller may be used on the panel simultaneously).

If relay controllers are fitted (other than TS0840), use a value greater than 0 where 1 represents every 8 relays available. For example:

- Enter 1 for one TS0841 8-Way Clocked Relay Card.
- Enter 2 for two TS0841 8-Way Clocked Relay Cards.
- Enter 2 for one TS0842 16-Way Open Collector Card.
- Enter 3 for one TS0841 8-Way Clocked Relay Card and one TS0842 16-Way Open Collector Card.
- Enter 4 for two TS0842 16-Way Open Collector Cards.

The numbering system allows for 32 relay controllers, which is considerably more than is practicable. In reality, the workable limit for a series of relays is about 144, which limits the number of 8-way relay controllers to a total of 18; or 16-way open collector cards to a total of 9. If more than 144 relays are required, it’s best to connect the additional relays via DGPs.

Number of Relay Controllers: 0
How Many:

Enter 0 if a TS0840 4-Way Relay Card is connected to the panel, and then press [ENTER]. Alternatively, enter a value greater than 0 where 1 represents every 8 relays available, and then press [ENTER].

Note: We recommend powering only one relay controller directly from the Challenger panel via the 10-way ribbon cable. Do not use the 10-way ribbon cable to power daisy-chained relay controllers.

Event text

When input types 57 (Input to report and screen) or 58 (Input to screen text) are active, the text specified here (up to 16 characters) is displayed on LCD RASs.

Event text:
(1)−Edit

To program a name via RAS, see “Programming text via RAS” on page 62.

Number of prefix digits

User PINs (four to ten digits long) may be used for both alarm control and access (door) control, depending on the setting of “Door event flag on alarm codes” on page 89.

The alarm code prefix value in the range one to four enables users to enter a door code (a shorter PIN) for access control.

For example, if a user’s full PIN is six digits long (for example, 123456), and the alarm code prefix value is 2, then the first two digits are removed for access control, and the user can operate doors by entering only the last four digits of the PIN (for example, 3456).

The door code must be at least four digits long. Table 12 below lists the prefix values that may be used for PINs of various lengths.

No Alarm Prefix
Prefix Len:

Enter the prefix value in the range one to four, and then press [ENTER].

Table 12: Acceptable ranges of alarm code prefix values

User PIN length (digits)	Alarm code prefix value	Resulting door code length
4	0	not applicable
5	1	4
6	1, 2	5, 4
7	1, 2, 3	6, 5, 4
8	1, 2, 3, 4	7, 6, 5, 4
9	1, 2, 3, 4	8, 7, 6, 5
10	1, 2, 3, 4	9, 8, 7, 6

Time before rotate

LCD RASs that have small displays (for example, 16-character LCD screens) scroll longer strings of text in order to display entire messages. This scrolling is referred to as ‘rotation’.

When a long message displays, the text rotation begins after a configurable delay. If you wish to change the delay time, enter a time value in the range 1 to 15 (a value of 0 uses the default delay time of 8).

Time Before Rotate is 0
Time:

Use a value in the range 1 to 7 for delay times less than default, or a value in the range 9 to 15 for delay times greater than default, and then press [ENTER].

Rotate speed

LCD RASs that have small displays (for example, 16-characters LCD screens) scroll longer strings of text in order to display entire messages. This scrolling is referred to as ‘rotation’.

When a long message displays, the speed of the text movement is configurable. If you wish to change the text speed, enter a time value in the range 1 to 15 (a value of 0 uses the default speed of 8).

Rotate Speed is 0
Time:

Use a value in the range 1 to 7 for more speed than default, or a value in the range 9 to 15 for less speed than default, and then press [ENTER].

User offset

This is not used by the Challenger*Plus* system.

EOL resistor

EOL Resistor Code: 0 − 10K Ohm
Code:

The Challenger system normally uses the default 10 kΩ End-Of-Lline (EOL) resistor value to detect the electrical states of input circuits. This option is used to apply a different EOL resistor value to the 16 zone inputs connected to the Challenger panel.

Enter a number to select the following EOL resistor values:

- Press [0] [ENTER] for 10K (default)
- Press [1] [ENTER] for 4K7
- Press [2] [ENTER] for 2K2
- Press [3] [ENTER] for 6K8
- Press [4] [ENTER] for 5K6
- Press [5] [ENTER] for 3K7
- Press [6] [ENTER] for 3K3
- Press [7] [ENTER] for 2K0
- Press [8] [ENTER] for 1K5

- Press [9] [ENTER] for 1K0
- Press [10] [ENTER] for 2K2/6K8 (see note below)

Press [ENTER] to return to the Install menu.

Time zone

```
Time Zone: 0 − NONE SET
Time Zone:
```

Challenger panels may be located in various remote regions. The time zone setting is used to indicate regional time zone (and DST combinations) when events are reported to the central monitoring station.

Enter a number to select the following time zone options:

- Press [0] [ENTER] for no time zone (default)
- Press [1] [ENTER] for Lord Howe Is. (UTC+10:30)
- Press [2] [ENTER] for Hobart TAS (UTC+10)
- Press [3] [ENTER] for Melbourne VIC (UTC+10)
- Press [4] [ENTER] for Sydney NSW (UTC+10)
- Press [5] [ENTER] for Broken Hill NSW (UTC+09:30)
- Press [6] [ENTER] for Brisbane QLD (UTC+10)
- Press [7] [ENTER] for Adelaide SA (UTC+09:30)
- Press [8] [ENTER] for Darwin NT (UTC+09:30)
- Press [9] [ENTER] for Perth WA (UTC+08)
- Press [10] [ENTER] for Eucla WA (UTC+08:45)
- Press [11] [ENTER] for New Zealand (UTC+12)

Press [ENTER] to return to the Install menu.

Area search TZ

```
Area Search Tz: 0
Enter Tz:
```

If Area Search functionality is required, enter the number of the soft or ‘hard’ time zone that will be used to trigger area search. See “Using Area Search” on page 56 for details.

Decrement test days during TZ

When using timed input testing (see “Using timed input testing” on page 61), you can assign a time zone in order to specify which days the system uses to check whether inputs have been tested. The default is time zone 0 (always valid).

```
Decrement test days during TZ 0
Enter TZ:
```

Enter the time zone (other than 0) that you defined to tell the panel what days of the week to use for timed input testing (for example, Monday through Friday).

External siren mode

Challenger*Plus* panels can support an 8 Ω external siren or an external device that requires 12 Volt DC power.

```
Ext siren mode: 0–Standard Siren
Siren Type:
```

Enter 0 for a standard 8 Ω siren or 1 for a DC Volts device, and then press [ENTER].

Warning: Specifying an external siren type of DC Volts when there is an 8 Ω external siren connected to the panel may damage the siren.

Internal siren mode

Challenger*Plus* panels can support an 8 Ω internal siren or an internal device that requires 12 Volt DC power.

```
Int siren mode: 0–Standard Siren
Siren Type:
```

Enter 0 for a standard 8 Ω siren or 1 for a DC Volts device, and then press [ENTER].

Warning: Specifying an internal siren type of DC Volts when there is an 8 Ω internal siren connected to the panel may damage the siren.

System options part 2

Input tamper monitoring

This setting determines whether the system can detect two input states (sealed and unsealed) or four input states (sealed, unsealed, open, and short). When input tamper monitoring is enabled, open or short conditions are both reported as an input tamper alarm (subject to input type, see “Input types” on page 229).

```
YES − Input Tamper Monitoring
*−Change 0−Skip
```

The following example is based on a system where every input has two end-of-line (EOL) resistors to enable the panel to detect whether an input is sealed, is in alarm, or is in tamper.

The default EOL resistor value is 10 kΩ, and the details below are based on the default. See “EOL resistor” on page *113*.

YES Input tamper monitoring is used:

Seal = 10 kΩ

In alarm = 5 or 20 kΩ

Fault = open or shorted.

NO Input tamper monitoring is not used:

Seal = 10 kΩ

In alarm = open or shorted or 5 or 20 kΩ

Note: Refer to the *ChallengerPlus Installation and Quick Programming Manual* for resistance values for all EOL resistor options.

Automatic deisolate when area accessed

NO − Auto Deisolate When Area Accessed
***−Change 0−Skip**

YES Inputs that are sealed and isolated are deisolated when any of the areas assigned to the inputs are disarmed.

NO Inputs that are sealed and isolated remain isolated (are not deisolated).

See also “Disable auto-deisolate” on page 101.

Display one input at a time

YES − Display One Input at a Time
***−Change 0−Skip**

YES One input at a time is displayed even though there may be more than one in the list of inputs to be displayed (the user must scroll through the inputs).

NO Inputs are displayed as a list of numbers and it is necessary to select the input number to display the input name.

Name file

Users’ names (up to 16 characters) for up to 2,000 users can be entered along with their PINs, when programming via an LCD RAS.

Note: If a TS1084 Memory Expansion Module is fitted to accommodate more than 2,000 users, then user names are not stored in the Challenger panel; they can be stored only in management software.

YES − Name File
***−Change 0−Skip**

YES Prompts for programming a user name are displayed when programming users.

NO When programming users the prompts for a user name are not displayed.

System alarms set siren and strobe

NO − System Alarms Set Siren & Strobe
***−Change 0−Skip**

YES The dedicated tamper inputs on the control panel and the DGPs activate the siren and strobe when in alarm.

NO The system alarms report and activate event flags only.

System alarms latch

System alarms are RAS/DGP offline, cabinet tamper, siren tamper, mains fail, fuse fail, and low battery.

```
NO − System Alarms Latch
*−Change 0−Skip
```

YES System alarms latch and require a code to reset.

NO System alarms automatically reset and report restoral when the alarm condition is no longer present.

Note: If set to YES, ensure that users who have the appropriate authority are assigned an alarm group that has “Reset system alarms” on page 100 set to YES.

Siren testing

```
NO − Siren Testing
*−Change 0−Skip
```

YES The sirens are tested for three seconds when the secure test is started (test mode 1 or 2).

NO The secure test is started without the Siren test.

See also “Test mode” on page 110.

Disable 0 [ENTER] for camera reset

```
NO − Disable 0 ENTER for Camera Reset
*−Change 0−Skip
```

YES 0 [ENTER] cannot be used to stop cameras operating after an alarm has occurred. The cameras continue to operate until an authorized user resets them.

NO 0 [ENTER] stops the cameras operating (after pressing [ENTER] [ENTER] for the Quick Alarm History. Refer to the *ChallengerPlus Administrators Manual* for details.

Disable insert of user category

```
NO − Disable Insert of User Category
*−Change 0−Skip
```

YES Disables the special procedure for automatically timing on non-vault areas when arming vaults.

NO Enables the special procedure for automatically timing on non-vault areas when arming vaults, provided all applicable values are programmed. See also “Option 18: Vaults” on page 169.

Disable of LEDs that don’t report

This is not used by the Challenger*Plus* system.

Disable code from displaying

```
NO − Disable Code From Displaying
*−Change 0−Skip
```

YES PINs are not visible in User menu 14 Program Users (except to master installer). The display shows “PIN codes cannot be viewed”.

NO PINs are visible.

Disable flashing area LEDs

```
NO − Disable Flashing Area LEDs
*−Change 0−Skip
```

YES The area LED will not flash on alarm or tamper.

NO The area LED will flash on alarm or tamper.

Dual custody code programming

```
NO − Dual Custody Code Programming
*−Change 0−Skip
```

YES Two users are required to enter their PINs before access is granted to program users (user 50, Master Code, is not required to have a second code to program users).

NO Validation is not needed when entering User menu 14, Program Users.

Display alarms instantly on LCD

```
NO − Display Alarm Instant On LCD
*−Change 0−Skip
```

YES Details of the first alarm are displayed instantly on the LCD RAS. Details of other alarms can be viewed on the LCD RAS by pressing [ENTER] [ENTER].

NO Details of all alarms can be viewed on the LCD RAS by pressing [ENTER] [ENTER].

Sirens only after report fail

```
NO − Sirens Only After Report Fail
*−Change 0−Skip
```

YES Siren event flags are activated on alarms, and report fail is registered, if the Challenger panel has failed to report to the remote monitoring company, as specified for the communication path’s dial settings. The siren activates for the normal siren cut-off time programmed. See “Report fail event flag” on page 185.

NO Sirens will operate on alarms.

Financial options

```
NO − Financial Options
*−Change 0−Skip
```

When enabled, the following special options apply (generally applicable to financial institutions):

- Film counters are enabled during the access test mode.
- Minimum PIN length is set to five digits.
- The area search procedure for financial institutions applies (see “Using Area Search” on page 56).

Display user flags

The special user flags are Dual Custody, Guard, Visitor, Trace User, Card Only, Privileged and Long Access.

```
NO − Display User Flags
*−Change 0−Skip
```

YES The special user flags are displayed in sequence after the floor group display when programming users.

NO The special user flags are not displayed.

Delay holdup lockout

This option is only applicable to latching delayed holdup alarms. If set to YES, an alarm can only be cancelled if the input is in sealed state. A latching holdup alarm is LOCKED OUT until the alarm device is taken out of its latched state (reset).

```
NO − Delay Holdup Lockout
*−Change 0−Skip
```

YES Delayed holdup alarm lockouts are enabled until the alarm device is reset.

NO Delayed holdup alarm lockouts are disabled.

Skip access check for service tech

```
NO − Skip Access Check for Service Tech
*−Change 0−Skip
```

YES Enables the User menu option 17. Enable Service Tech to be used when the system is armed.

NO All areas must be disarmed before the option can be used to enable service technician access.

Enable expanded test reporting

NO − Expanded Test Reporting
***−Change 0−Skip**

YES Enables the use of the “Test Input Within No. of Days” functionality (timed input testing), which is programmed individually for inputs. This option provides system-wide control over this functionality.

NO Timed input testing not used.

Expanded test success reporting

NO − Expanded Test Success Reporting
***−Change 0−Skip**

YES When timed input testing is used (Expanded Test Reporting set to Yes), and an input is tested within its specified number of days, enable this option to send a test success message (CID 611 ‘Point tested OK’) for the input number.

NO Timed input test success messages are disabled.

Enable exit fault reporting

NO − Exit Fault Reporting
***−Change 0−Skip**

YES Exit fault reporting is used to indicate to the alarm reporting centre that an unsealed input has gone into “exit error alarm” (CID 374) by being unsealed when the exit timer is running. This is typically caused by a user arming the system when inputs are not sealed, as permitted by the user's Alarm Group option “Forced arming when inputs unsealed” on page 102. The exit timer suppresses alarms from entry/exit input types (3, 4, 13, 14, 41, and 42) but does not suppress alarms from other inputs. FIXME [Does this apply to new input types 61 and 62?]

NO If exit fault reporting is not used, or if the input is still unsealed after the exit timer expires, then the input's programmed CID code is reported.

Enable V8 multibreak

By default, Challenger*Plus* reports multi break input alarms as CID 139 Burglar alarm, Intrusion verifier. If the “Multi break alarms” option is set to YES for any Comm path, you can choose to report multi break alarms in the same manner as a Challenger V8 panel (as a multi break event on the input’s programmed CID code).

NO − Enable V8 Multibreak
***−Change 0−Skip**

Press [*] - toggle the YES and NO value. Press [ENTER] - move to the next option.

Enable V8 numbering

Challenger*Plus* uses the latest numbering system, but is able to use the V8 input numbering system if required. If this option is set, Challenger will use V8 input numbering.

```
NO − Enable V8 Numbering
*−Change 0−Skip
```

Press [*] - toggle the YES and NO value. Press [ENTER] - move to the next option.

System options part 3

Site Code A

This is not used by the Challenger*Plus* system.

Offset A

This is not used by the Challenger*Plus* system.

Site Code B

This is not used by the Challenger*Plus* system.

Offset B

This is not used by the Challenger*Plus* system.

Card learn RAS

A card reader RAS can be used to enter a user’s card data (card bits) into the Challenger system by presenting (badging) the card at the reader during the user creation process via RAS, not via management software.

```
Card Learn RAS: 1
Enter RAS:
```

Enter the card reader’s RAS address in the range 1 to 16 or 65 to 80, and then press [ENTER]. The default setting is RAS 1.

Option 8: Auto reset

This function is used to program the Challenger to automatically reset alarms. The auto reset functionality is typically used for specified areas, and during specified times (for example, at night), each of which is determined by an alarm group.

Note: It may be necessary to program a special alarm group for this function.

A worksheet is provided to record programming details and to further describe this option. See “

Auto reset worksheet” on page 261.

Auto reset time

Auto reset time is the amount of time that elapses between the alarm occurring and the alarm reset attempt.

```
Auto Reset Disabled
Time (Mins):
```

Enter the amount of time (1 to 255 minutes), and then press [ENTER]. Enter 0 to disable auto reset.

Reset alarm group

An alarm group tells the control panel which areas to auto reset, and the alarm group’s time zone tells the control panel the times that this may occur.

```
Reset Alm−Grp: 1−No Access
Alm−Grp:
```

Enter the code for the alarm group, and then press [ENTER].

Option 9: Communications

A set of three worksheets is provided to record programming details and to further describe this option. See:

- “Figure 40: Communications devices worksheet (onboard hardware)” on page 263 and “Figure 41: Communications devices worksheet (external hardware)” on page 264 for the hardware setup.
- “Figure 42: Communications paths worksheet” on page 265 for setting up Paths.

Each of the worksheets is sectioned into areas that correspond to the tabs in the CTPlus software set up screens.

This option is used to set up the Challenger panel’s communications hardware and paths, and to check the status of communications paths.

```
1−Setup H/W 2−Setup Paths 3−Status 4−UltraSync
0−Exit, Menu:
```

Refer to the following sections for details about these options:

- Press [1] [ENTER] for “Setting up communications hardware” on page 123
- Press [2] [ENTER] for “Setting up communications paths” on page 129
- Press [3] [ENTER] for “Checking communications status” on page 150
- Press [4] [ENTER] for “UltraSync” on page 153

Setting up communications hardware

From the Communications menu, “Option 9: Communications” on page 122, press [1], and then press [ENTER].

```
Setup Menu
0−Exit, Menu:
```

Press [ENTER] to see each of the hardware setup menu options in turn:

- Press [1] [ENTER] to set up onboard devices
- Press [2] [ENTER] to set up a device in expander slot 1
- Press [3] [ENTER] to set up a device in expander slot 2
- Press [4] [ENTER] to set up a device in expander slot 3

The first option is described in “Setting up the panel’s onboard devices” below.

Note: Various devices can be mounted in the panel’s three expander slots, and the programming options vary. Refer to the device’s installation instructions for set up instructions.

Setting up the panel’s onboard devices

From the Setup menu, “Setting up communications hardware” above, press [1], and then press [ENTER] to configure the panel’s onboard ports for RS-232 via J15 (STU), Ethernet, modem, and USB.

The programming options displayed might not relate to the device you are setting up. For example, the first option is specific to the onboard modem. Skip any items that do not apply.

Modem options

Monitor ring

When this option is enabled, the Challenger panel watches for ringing at the onboard modem. When the programmed number of rings and number of calls are met, then the modem can connect.

```
NO−Monitor Ring
*−Change 0−Skip
```

Change the value if needed, or press [ENTER] to move to the next option.

Enable Blind Dial

When this option is enabled, the onboard modem’s dial tone detection is disabled. This allows the Challenger panel to dial regardless of whether the modem detects a dial tone.

```
NO−Enable Blind Dial
*−Change 0−Skip
```

Change the value if needed, or press [ENTER] to move to the next option.

Line fault monitoring

When this option is enabled, the Challenger panel watches for a fault on the line, such as voltage lost. If a fault is detected, then a line monitor fail alarm is triggered.

```
NO−Enable PSTN Line Fault Monitor
*−Change 0−Skip
```

Change the value if needed, or press [ENTER] to move to the next option.

Enable New Zealand dialling

When this option is enabled, the Challenger panel’s modem uses dial tones compatible with New Zealand standards.

```
NO−Enable New Zealand Dialling
*−Change 0−Skip
```

Change the value if needed, or press [ENTER] to move to the next option.

Serial options

Baud rate

```
STU Baud Rate 8−57600
No:
```

If you are connecting to the Challenger panel via J15 (STU), enter a number to select the following baud rates:

- Press [0] [ENTER] for disabled
- Press [1] [ENTER] for 300 baud
- Press [2] [ENTER] for 1200 baud
- Press [3] [ENTER] for 2400 baud
- Press [4] [ENTER] for 4800 baud
- Press [5] [ENTER] for 9600 baud
- Press [6] [ENTER] for 19200 baud
- Press [7] [ENTER] for 38400 baud
- Press [8] [ENTER] for 57600 baud (default)

Press [ENTER] to move to the next option.

Parity

```
STU Parity: None
*−Change 0−Skip
```

When connecting to the Challenger panel via J15 (STU), press [*] to toggle between the values of none, odd, and even parity.

Press [ENTER] to move to the next option.

Stop bits

```
STU Stop Bits: 1 Bits
*−Change 0−Skip
```

When connecting to the Challenger panel via J15 (STU); press [*] to toggle between the values of 1 and 2 bits.

Press [ENTER] to move to the next option.

USB options

USB options

```
USB:Device
*−Change 0−Skip
```

Pressing [*] toggles between the values of host and slave/device. The slave/device setting is used when you are connecting the Challenger panel to a management software computer via USB.

Press [ENTER] to move to the next option.

Ethernet options

Enable Ethernet

```
NO−Ethernet
*−Change 0−Skip
```

For Ethernet connection via any path, press [*] to toggle the YES and NO values (enabled and disabled).

Note: Change this value to YES if connecting to management software or IP Receiver via Ethernet.

Press [ENTER] to move to the next option.

Enable DHCP

If the ChallengerPlus panel is on a network where devices are assigned addresses via DHCP, this option can be enabled to automatically retrieve an IP address. Setting this to ‘No’ will require that settings are entered manually instead. DHCP is configured to be enabled by default on a ChallengerPlus panel, unless upgrading from a Challenger10 panel.

```
YES−Enable DHCP
*−Change 0−Skip
```

Press [ENTER] to move to the next option.

Enable ping

Ping should only be enabled as an aid to configuring the system, and disabled at other times.

```
YES−Enable Ping
*−Change 0−Skip
```

For Ethernet connection via any path, press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

If DHCP has been enabled in the previous steps, you will be presented with a screen telling you where to find IP info.

```
See menu 19/9/3/2/1 for IP info
Press ENTER
```

Otherwise, you will need to manually configure these settings using the instructions below.

IP address

```
IP Add: 192.168.000.117
IP(1):
```

For Ethernet connection via any path, use the panel’s default IP address initially, or a custom IP address assigned by the site’s network administrator, as required.

Press [nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER] to program the Challenger IP address provided by the network administrator. nnn represents a portion of the assigned address from 000 to 255.

Tips:

- Use the up and down arrow keys or buttons to jump between numbered octets.
- Press [0]-[ENTER] to program a 000 segment. Leading zeros are not required.

Subnet mask

```
Subnet Mask: 255.255.255.000
IP(1):
```

For Ethernet connection via any path, use the default subnet mask, or a mask assigned by the site’s network administrator.

Press [nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER] to program the subnet mask. The “nnn” represents a portion of the mask from 000 to 255.

Tips:

- Use the up and down arrow keys or buttons to jump between numbered octets.
- Press [0]-[ENTER] to program a 000 segment. Leading zeros are not required.

Gateway address

```
Gateway Add: 000.000.000.000
IP(1):
```

For Ethernet connection via any path, you may need to enter a gateway address assigned by the site’s network administrator.

Press [nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER] to program the gateway address. nnn represents a portion of the assigned address from 000 to 255.

Tips:

- Use the up and down arrow keys or buttons to jump between numbered octets.
- Press [0]-[ENTER] to program a 000 segment. Leading zeros are not required.

DNS address 1

```
DNS 1 Add: 000.000.000.000
IP(1):
```

For UltraSync connection via an Ethernet link path, enter a primary DNS address assigned by the site’s network administrator. See “Connecting via UltraSync” on page 67 for more information.

Press [nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER] to program the primary DNS address. nnn represents a portion of the assigned address from 000 to 255.

Tips:

- Use the up and down arrow keys or buttons to jump between numbered octets.
- Press [0]-[ENTER] to program a 000 segment. Leading zeros are not required.

DNS address 2

```
DNS 2 Add: 000.000.000.000
IP(1):
```

For UltraSync connection via an Ethernet link path, enter a secondary DNS address assigned by the site’s network administrator. See “Connecting via UltraSync” on page 67 for more information.

Press [nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER] to program the secondary DNS address. nnn represents a portion of the assigned address from 000 to 255.

Tips:

- Use the up and down arrow keys or buttons to jump between numbered octets.
- Press [0]-[ENTER] to program a 000 segment. Leading zeros are not required.

Setting up external devices

From the Setup menu, “Setting up communications hardware” on page 123, press [2] or [3], and then press [ENTER] to configure the respective expander. The programming options displayed depend on the type of expander module fitted. This module is auto-detected on the ChallengerPlus panel to simplify the required configuration, and is shown on the LCD screen when selecting the hardware location. A star next to the device name indicates that it is enabled.

```
2-EXP1-TS1054 *
0-Exit, Menu:
```

3G & 4G Communication Module

Up to 2 SIMs may be installed in the communications module. For each connected SIM card the following information must be programmed into the system.

Note that the SIM 2 Options are not supported on the TS1053.

Enable hardware

The expander may be enabled or disabled for use on the ChallengerPlus panel. The first part of each segment will show the expander number being configured, as “E(n)”, where “(n)” is the expander number. In the example below, we are configuring Expander 1, so this is displayed as “E1”.

```
E1:YES-Enabled
0-Exit, Menu:
```

Press the * button to toggle whether the expander is enabled or disabled.

SIM PIN

Type the Personal Identification Number (PIN) for the SIM card in the module’s SIM slot.

SIM APN

The Access Point Name (APN) is input for the SIM card in the module’s SIM slot.

APN Username

Type the APN user name (if required) for the SIM card in the module’s SIM slot.

APN Password

Type the APN user name (if required) for the SIM card in the module’s SIM slot.

SIM APN Authentication

From the list given below, select the type of authentication required for the SIM card in the module’s SIM slot.

The types of authentication available are:

- **0-None.** Select this option if no authentication is to be used.
- **1-PAP.** Select PAP (Password Authentication Protocol) if this is the authentication type.
- **2-CHAP.** Select CHAP (Challenge Handshake Authentication Protocol) if this is the authentication type.

Setting up communications paths

From the Communications menu, “Option 9: Communications” on page 122, press [2], and then press [ENTER].

```
Enter Comm Path: None
0−Exit, No:
```

Press [nn]-[ENTER] to configure a communications path. nn represents a path number from 1 to 10. Paths 4 through 9 are not preconfigured. Any path may be configured as required.

The following paths have default values:

- Path 1–CID Dialler is for modem connection to central station CID reporting.
- Path 2–USB INSTALLER is for USB connection to an installer’s computer for installation programming.
- Path 3–MANAGEMENT SOFT is for IP connection to a management software computer.
- Path 10–SERVICE is for use with User menu option 7 Service Menu, when a temporary dialler connection to management software is required.

Setting up a path

This section describes how to configure communications path 3 for IP connection to a management software computer. The process for other paths is similar, but details will vary.

From the Enter Comm Path prompt, “Setting up a path” above, press [3], and then press [ENTER].

```
Enter Comm Path: 3−MANAGEMENT SOFT
0−Exit, No:
```

Tip: The path name is followed by an asterisk (*) when the path is enabled.

Press [ENTER] to access the path setup menu.

```
P3:1−Path Main
0−Exit, Menu:
```

Press [ENTER] to see each of the path setup menu options in turn. The path setup options are described in the following sections.

- “1–Path main” below
- “2–Path Connection Control” on page 135
- “3–Path Filter” on page 137
- “4–Path Test Calls” on page 140
- “5–Path Dial Settings” on page 141
- “6–Path IP Address” on page 144
- “7–Path Encryption Settings” on page 146
- “8–Path Advanced Settings” on page 146
- “9–Reset Path Queues” on page 149
- “10–Path Authentication” on page 149

The programming options displayed might not relate to the path you are setting up. For example, dial settings is specific to modems. Skip any items that do not apply

1–Path main

Format

From the path setup menu - see “Setting up a path” on page 129 - press [1], and then press [ENTER] to select a communications format. The top line of the RAS begins with the number of the path being programmed (for example, “P3”).

```
P3:Format:3−Computer Event
Format No:
```

Each communications path must be assigned a format. Table 13 below lists the relationship between formats and hardware.

Table 13: Communications formats by device type

Formats/Devices	Dialler	STU (RS-232)	IP/3G module	USB
1–Contact ID Modem	Yes	No	No	No
2–Computer Polled	Yes	Yes	Yes	Yes
3–Computer Event	No	No	Yes	No
4–IP Receiver	No	No	Yes	No
5–Securitel STU	No	Yes	No	No
6–Printer	No	Yes	Yes	No

Formats/Devices	Dialler	STU (RS-232)	IP/3G module	USB
7–CBus	No	Yes	Yes	No
8–DVMRE Time Stamp	No	Yes	No	No
9–IP Receiver Names	No	No	Yes	No
10–Mobile	No	No	Yes	No
11–UltraSync	No	No	Yes	No

Enter a number to select the following communications formats:

- Press [0] [Enter] for none
- Press [1] [Enter] for Contact ID Modem.
  A sub-format menu display appears: 0–None or 1–Contact ID Hex may be selected.
- Press [2] [Enter] for Computer Polled
- Press [3] [Enter] for Computer Event
- Press [4] [Enter] for IP Receiver. A sub-format menu display appears: 0–None or 1–Contact ID Hex may be selected. For information about CID hex formats, see “TS-CHPLUS CID CODES” excel sheet.
- Press [5] [Enter] for Securitel STU. A sub-format menu display appears: 0–None, 1–STU Contact ID, or 2–STU Contact ID Hex may be selected. (STU Contact ID or STU Contact ID Hex can be used when communicating to external receivers that support the TECOM STU format.)
- Press [6] [Enter] for Printer. A sub-format menu display appears: 0–None, 1–HP Laser, 2–Epson, or 3–Debug may be selected. (Use the debug option only if instructed to by Technical Support.)
- Press [7] [Enter] for C-Bus
- Press [8] [Enter] for DVMRE Time Stamp (not supported in this release)
- Press [9] [Enter] for IP Receiver Names
- Press [10] [Enter] for Mobile device
- Press [11] [Enter] for an UltraSync link path. This option is not currently supported through this menu, UltraSync must be configured using “UltraSync” setup in the communications menu. See “Connecting via UltraSync” on page 67 for more information about UltraSync.

After you select a format, many of the subsequent options are pre-programmed with values appropriate to that format.

Note: If you need to change the format of a path that has been previously programmed (or one of the default paths), first set the format to “0–None” to clear the previous format’s programming.

In the following example, communications path 3 uses format 3–Computer Event by default for UDP/IP event-driven connection to a management software computer.

Press [ENTER] to move to the next option.

Enable path

```
P3:NO−Enabled
*−Change 0−Skip
```

If you are connecting to the Challenger panel via Ethernet, press [*] to toggle the YES and NO values (enabled and disabled).

Note: Change this value to YES if connecting to management software via Ethernet.

Press [ENTER] to move to the next option.

Path name

```
P3:Name:MANAGEMENT SOFT,(1)−Edit
MANAGEMENT SOFT
```

Press [ENTER] to accept the default name and move to the next option. Alternatively, press [1] to change to text edit mode.

```
P3:Name:MANAGEMENT SOFT,(*)−End
MANAGEMENT SOFT
```

To assign a custom name to the path, use the keypad to enter the name. Refer to Table 5 on page 62 or “Entering text via RAS” in the *ChallengerPlus Administrators Manual* for details.

Press: [*] - move to the next option.

Path location

```
P3:Select Location 1−Onboard
Option:
```

Enter a number to select the following location options:

- Press [1] - Onboard if the path communicates via the panel’s onboard hardware.
- Press [2] - EXP1 if the path communicates via the first expander module.
- Press [3] - EXP2 if the path communicates via the second expander module.
- Press [4] - EXP3 if the path communicates via the third expander module.
- Press [5] if the path communicates via an existing UltraSync link path. See “Connecting via UltraSync” on page 67 for more information.

Press: [*] - move to the next option.

Path slot

After selecting a hardware location, you need to indicate which slot (port) on the hardware the path will use. The options will vary depending on the hardware. The following example is based on location 1–Onboard.

```
P3:Slot is set to 2−Ethernet
Option:
```

Enter a number to select the following slot (port) options:

- Press [0] for none (disabled).
- Press [1] for RS232-STU if this path uses the panel’s J15 connector.
- Press [2] for Ethernet if this path uses the panel’s Ethernet port.
- Press [3] for Modem if this path uses the panel’s RJ-12 socket.
- Press [4] for USB if this path uses the panel’s USB port.

Note: The above option numbers relate only to location 1–Onboard. Other locations may have their slots named and numbered differently.

Press: [*] - move to the next option.

Account code

```
P3:Account Code Is 0001
Acc:
```

Account code is used in two ways, depending of what this path is used for:

- If connecting to a management software computer, type a number in the range 1 to 1024 to match the computer address.
- If reporting to central station via DTMF dialler, type the four-digit account number provided by that monitoring company that identifies your system to the monitoring company. If not used, enter 0000.

Press: [*] - move to the next option.

Priority

```
P3:Priority over other paths is: 0
Priority No:
```

If the path uses the dialler, click the arrow, and then select a priority number in the range 1 to 10 (the highest priority being 1), or 0 for no priority assignment.

Press: [*] - move to the next option.

Priorities are only relevant to Comm Paths using the modem port. A higher priority (lower priority number) comm path will cause a lower priority path to disconnect if it needs to use the modem.

Backup for path number

```
P3:Backup For Path No: None
Path No:
```

A path can be designated as a backup for another path. For example, you can program two paths for the same purpose so that if the connection via the primary path is lost then the secondary path takes over until the primary path is restored.

Two levels of backup are supported. For example path 1 can be a backup for path 2, which can be a backup for path 3. So, if path 3 can't communicate, then the panel tries path 2. If paths 3 and 2 can't communicate, then the panel tries path 1.

Notes:

- When a backup path is active, events will be reported according to the backup path’s filtering options such as areas, time zones, and so on. We do not recommend using one type of path format to backup a different type of path format due to varied filtering options (for example, using a CID Dialler path as a backup for Management Software path).
- When using a CID Dialler path as a backup, the dialler will not connect until triggered by an alarm event even if the path it backs up is configured to always connect.

Enter the number of the path that this path backs up. Enter 0 if this path does not back up another path. Press: [*] - move to the next option.

Computer password

There are two methods for authenticating a connection from a remote computer to a Challenger system:

- Computer password
- Path authentication with user name and password

The default method is computer password, as defined by this option. See “10–Path Authentication” on page 149 for information on configuring the path authentication method.

```
P3:Computer Password is: 0000000000
Pass:
```

The Challenger system requires a security password before granting access to a remote computer. Security passwords are always 10 digits. The default is 0000000000. A management software computer with any 10-digit password can connect to a Challenger panel that has a default password. The management software password will be saved to the path upon connection.

Note: The management software computer can always connect to the control panel with the default password except when connecting via the dynamic computer IP address option (see “Dynamic computer IP address” on page 145), in which case, a non-zero password is required.

Enter the password, and then press [ENTER].

2–Path Connection Control

From the path setup menu - Setting up a path on page 129 - press [2], and then press [ENTER].

Always connect

This option enables the path to remain constantly connected. In the case of a dialler path, the panel will only disconnect if a path programmed with a higher priority (such as CID reporting) needs to make a connection via dialler. When the higher priority task is finished, this path will reconnect.

```
P3:YES−Always Connect
*−Change 0−Skip
```

Press [*] - toggle YES / NO values.

Note: Change this value to YES if connecting to management software via USB or Ethernet, or for connecting to a printer.

Press [ENTER] - move to the next option.

Connect on event

This option enables path to initiate a connection when an alarm event or an access event triggers it.

```
P3:NO−Connect on Event
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Connect on service

This option must be enabled in order to dial the telephone number recorded in “First telephone number” on page 142 when requested via User menu 7 Service Menu.

```
P3:NO−Connect on Service
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Connect on buffer at 80%

This option enables path connection when the events buffer is 80% full.

```
P3:NO−Connect on Buffer at 80%
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Isolated inputs trigger path

This option applies to paths that report via dialler and an applicable connection option is also enabled (for example, “Connect on event”). When enabled, the path reports when inputs are isolated.

```
P3:NO−Isolated Inputs Trigger Path
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Note: “Report alarm events” must be enabled for this option to work.

Stay connected on empty buffer

This option applies to paths that report via dialler and maintains path connection after all events have been sent. The panel will only disconnect if a path programmed with a higher priority (such as CID reporting) needs to make a connection.

```
P3:YES−Stay Connect on Empty Buffer
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Control command

This option enables this path to control Challenger devices via a remote computer (for example, to open a door).

```
P3:YES−Control Command
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Trigger comms fail event

Select this option to trigger the report fail event flag, and report via RAS, if this path fails.

```
P3:NO−Trigger Comms Fail Event
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Use Area account codes

This option enables this path to use the area account code that is programmed for an area when reporting to central station.

```
P3:NO−Area Account Codes
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Communications Event triggers path

When enabled, this path is triggered to connect when an Ethernet heartbeat fail condition is detected.

```
P3:NO−Communications Event triggers Path
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

3–Path Filter

From the path setup menu - “Setting up a path” on page 129 - press [3], and then press [ENTER].

Filter event to area

This option enables this path to filter (restrict) the events reported to either a specified area or area group. If no area or area group is selected, the events from all areas are reported on this path.

```
P3:Filter Event to Area: 0
'*'−Grp, Area:
```

Enter an area number or an area group number (depending on your entry mode), and then press [ENTER].

Event time zone

This option enables this path to report events based on a ‘hard’ time zone or a soft time zone (time zone to follow relay).

```
P3:Event TimeZone: 0
No:
```

Enter a time zone number, and then press [ENTER].

Multi break alarm timer

If the “Multi break alarms” option is set to YES, you can define a time (0 to 255 seconds) to prevent ‘old’ multi break input alarms from being reported. For example, if you program a value of 30 seconds, then only multi break alarms that are less than 30 seconds old will be reported.

```
P3:Multi break alarm timer: 0
Time:
```

Enter the number of seconds, and then press [ENTER].

Note: This option does not apply if “Enable V8 multibreak” on page 120 is set to Yes.

Report alarm events

This option enables this path to report alarm events.

```
P3:YES−Report Alarm Events
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Report access events

This option enables this path to report access events.

```
P3:YES−Report Access Events
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Send events out of TZ

This option enables this path to report events only when the selected time zone is invalid.

```
P3:NO−Send Events out of TZ
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Remove unsent events

Events may be reported only during a specified time zone (or only outside of a specified time zone, if Send Event out of TZ is selected).

Enable this option (YES) if you want to ignore events when they are not being reported due to time zone settings. Events that are not reported will be discarded (not stored in the path's queue).

If not enabled (NO), then the unsent events are stored in the path's queue. When the time zone allows reporting, then the events from the queue are sent (along with any new events).

```
P3:NO−Remove Unsent Events
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

System alarm report

This option enables this path to report system alarm events. System alarms include all alarm events that are not associated with an area.

```
P3:YES−A00:System Alarm Report
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Note: “Report alarm events” must be enabled for this option to work.

Multi break alarms

This option controls how this path reports multiple alarms from one input to the remote monitoring company.

```
P3:YES−Multi Break Alarms
*−Change 0−Skip
```

When enabled, and an individual input alarms more than once before being reset by a user, each alarm is reported to the remote monitoring company.

If not enabled, and an individual input alarms more than once before being reset by a user, then only the first alarm is reported to the remote monitoring company.

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Note: “Report alarm events” must be enabled for this option to work.

Multi break restores

This option controls how this path reports multiple alarm restorals from one input to the remote monitoring company.

```
P3:YES−Multi Break Restores
*−Change 0−Skip
```

When enabled, and an individual input alarm is restored more than once before being reset by a user, each restoral is reported to the remote monitoring company.

If not enabled, and an individual input is restored more than once before being reset by a user, then only the last restoral is reported to the remote monitoring company.

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Note: “Report alarm events” must be enabled for this option to work.

Report open/close

This option enables this path to report when all areas (or areas specified in “Filter event to area” on page 137) open and close (are disarmed and armed).

```
P3:YES−Report Open/Close
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Note: “Report alarm events” must be enabled for this option to work.

Common open/close

When selected (and Report Open/Close is selected), this option causes the path to report open when the first reporting area is disarmed, and closed when the last reporting area is armed. In both cases, the lowest reporting area number (circuit number) is used, regardless of when that area was disarmed or armed.

If not enabled, but Report Open/Close is enabled, then this path will report open or close whenever a programmed area is armed or disarmed.

```
P3:NO−Common Open/Close
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Report computer connected

This option enables the “computer connected” event to be generated when a remote computer has connected to the panel via this path. This event can then be reported via your central station reporting path.

```
P3:NO−Report Computer Connected
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Report communication event

This option enables this path to report communications events.

```
P3:YES−Report Communications Events
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

Notes:

- This option must be set to NO if this path is used for reporting to a central station or an IP Receiver.
- This option does not apply if the path format is 10–Mobile.

Disarm clears pending alarms

This option enables this path to clear pending input alarms from history when an area is disarmed.

```
P3:NO−Disarm clears pending alms
*−Change 0−Skip
```

Press [*] - toggle YES / NO values. Press [ENTER] - move to the next option.

4–Path Test Calls

This option determines whether the Challenger panel activates test calls to the monitoring company and, if so, how often. The test call ensures that communications are operating correctly and can be programmed to only be made if there have been no events to initiate a call since the last test call.

From the path setup menu - Setting up a path on page 129 - press [4], and then press [ENTER].

Test call option

```
P3:Test Calls − None
Option:
```

Enter a number to select the following test call options:

- Press [0] [ENTER] for none (disabled).
- Press [1] [ENTER] for daily test calls.
- Press [2] [ENTER] for weekly test calls.

- Press [3] [ENTER] for daily test calls if no events.
- Press [4] [ENTER] for weekly test calls if no events.
- Press [5] [ENTER] for four-hourly test calls.
- Press [6] [ENTER] for four-hourly test calls if no events.
- Press [7] [ENTER] for hourly test calls.
- Press [8] [ENTER] for hourly test calls if no events.

Hours

Enter the hours in the range 0 to 23, press [ENTER], and then press [ENTER].

```
P3:Send a Test Call at 00:00 Sunday
Hours:
```

Minutes

Enter the minutes in the range 0 to 59, press [ENTER], and then press [ENTER].

```
P3:Send a Test Call at 06:00 Sunday
Minutes:
```

Day

For weekly test calls, enter the day needed, and then press [ENTER]. For the days of the week, enter their numerical value with Sunday as “1” and Saturday as “7”.

```
P3:Send a Test Call at 06:30 Sunday
(1)Sun−(7)Sat:
```

5–Path Dial Settings

From the path setup menu - Setting up a path on page 129 - press [5], and then press [ENTER].

Different paths can use a different telephone numbers, depending on the path’s purpose. For example, you might have different paths for:

- Connection to a management software computer.
- Reporting to a monitoring company.
- Service connection to a remote computer for programming (the telephone number that will be dialled by the system if the user menu option 7–Service Menu is set to option 3–Dial Management Software).
- Call-back connection to a remote computer for programming (the telephone number that will be dialled by the system when it detects a call-back trigger).

Note: For Challenger panels used in regions that are subject to New Zealand Telecoms authority, you must comply with “This product conforms to the standards set by Standards Australia on behalf of the Australian Communications and Media Authority (ACMA). We recommend enclosure covers remain fitted to maintain ACMA compliance.

Regulatory requirements for New Zealand” on page v.

PABX Number

```
P3: '*'–Pause, Ph No:
PABX:
```

If required, enter a PABX access code (for example, if you must dial 9 to get an outside line). This record is optional and may be omitted if the system is not connected via the switchboard. Other uses for this record include:

- Area code for STD telephone numbers.
- Satellite access code for remote locations.

Enter the dialling sequence required and press [ENTER].

Key sequences are used to enter additional characters after the PABX access code. Using a PABX access code “9” for example, the following additional characters may be added:

- The sequence [9] [MENU*] [MENU*] [ENTER] produces “9P” for a 2-second pause after dialling the 9. We recommend including one or two pauses after the PABX number.
- The sequence [9] [MENU*] [ENTER] produces “9#”. Certain PABX systems and telephone networks require the ‘#’ character to invoke special behaviour (use only if needed).

If a telephone number has been previously entered, it may be cleared by pressing [MENU*] [MENU*]. A “P” will now appear on the lower line of the display and the previously entered telephone number will appear on the top line of the display. Press [ENTER] and the number will be cleared.

First telephone number

```
P3: '*'–Pause, Ph No:
Ph1 No:
```

Enter the first telephone number that the system will attempt to call (by the value programmed in “Number of redials” below) in response to, for example, an alarm event. Press [ENTER] to move to the next option.

Second telephone number

```
P3: '*'–Pause, Ph No:
Ph2 No:
```

Enter the second telephone number that the system will attempt to call in response to, for example, an alarm event, if it fails to report via the first phone number. Press [ENTER] to move to the next option.

Number of redials

```
P3:Number of Redials is 0
No:
```

Enter the number of redial attempts that the system will make when the initial dialling attempt has failed.

Press [ENTER] to move to the next option.

If connection is not made after the programmed number of redials on all phone numbers, then this path’s nominated backup path is triggered.

If other events occur during the failed connection attempt, then the panel will restart the connection process (repeating all redial attempts, if necessary) for a second, and then a third time. If it can’t report after three rounds, then it fails to report and doesn’t try again until a new event occurs.

Number of calls to answer

```
P3:Number of Calls to Answer is 0
No:
```

Enter the number of detected calls that are required before the system answers or initiates a call back. Press [ENTER] to move to the next option.

Number of rings to answer

```
P3:Number of Rings to Answer is 0
No:
```

Enter the number of rings that are required before a call is detected. A telephone ring tone that consists of a double tone (brrr-brrr) is counted as two rings.

Auto answer

This option enables this path to be used to answer incoming calls after the number of rings and the number of calls are met.

```
P3:NO−Auto Answer
*−Change 0−Skip
```

Press [*] - toggle the YES / NO values. Press [ENTER] - move to the next option.

Call back

This option enables this path to be used by the panel to dial the telephone number of a remote PC, when it detects a call-back trigger. Program the telephone number as this path’s “First telephone number” on page 142.

```
P3:NO−Call Back
*−Change 0−Skip
```

Press [*] - toggle the YES / NO values. Press [ENTER] - move to the next option.

DTMF dial

```
P3:NO−DTMF Dial
*−Change 0−Skip
```

Enable this option if you want the path to use DTMF Tone dialling. If not selected, then decadic dialling will be used.

Press [*] - toggle the YES / NO values. Press [ENTER] - move to the next option.

6–Path IP Address

From the path setup menu - Setting up a path on page 129 - press [6], and then press [ENTER].

This path can connect via IP to a remote computer via:

- A programmed computer IP address (see “Send to IP address” below).
- A dynamically assigned computer IP address (see “Dynamic computer IP address” on page 145).

Send to IP address

The Challenger panel can use this IP path to connect to a remote computer, IP Receiver, or other supported software, via:

- An Ethernet cable from the Challenger panel’s Ethernet port. In this case you need to use the IP address of the remote computer.
- A Cellular (wireless) connection from a TS1054 4G Communication Module fitted to one of the Challenger panel’s expander slots. In this case you need to use the IP address of the WAN to access the data carrier’s access point (mobile internet).

```
P3:IP Add: 000.000.000.000
IP(1):
```

Press [nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER]-[nnn]-[ENTER] to program the IP address of the remote computer (or WAN, in the case of a TS1053 3G Communication Module), where nnn represents a portion of the assigned address from 000 to 255.

Tips:

- Use the up and down arrow keys or buttons to jump between numbered octets.
- Press [0]-[ENTER] to program a 000 segment. Leading zeros are not required.

You do not need to program an IP address for this path if “Dynamic computer IP address” on page 145 is enabled.

Send IP Port

```
P3:Send IP Port is 0000
No:
```

Enter the port number (for example, 3001) that will be used for sending data to other devices, and then press [ENTER].

Listen IP Port

```
P3:Listen IP Port is 0000
No:
```

Enter the port number (for example, 3001) that will be used for receiving requests from other devices, and then press [ENTER].

IP mode

```
P3:UDP/IP
*−Change 0−Skip
```

Select UDP/IP if you want the Challenger panel to communicate in event-driven mode with management software, as well as to IP Receiver. In event-driven mode the Challenger panel reports events only as they occur. This prevents the management software and IP Receiver software from continuously polling Challenger panels and therefore minimises network bandwidth requirements.

Select TCP/IP if you want the Challenger panel to communicate in polled mode with management software. Polled mode typically consumes greater bandwidth than event-driven mode. However, this can be useful for panels that deliver little event-driven activity. Some networks require a certain amount of activity in order to maintain an active communications path.

Press [*] - toggle the modes. Press [ENTER] - move to the next option.

Server/Client mode

```
P3:Server
*−Change 0−Skip
```

If TCP/IP is used, you can configure whether the panel acts in a server or a client capacity. The default setting is server: change it to client for TCP/IP auto-enrol functionality.

Dynamic computer IP address

```
P3:NO−Dynamic Computer IP Address
*−Change 0−Skip
```

When enabled, this path will allow an IP connection from a computer at any IP address where:

- The connection request is received via the correct port number.
- The path’s (non-zero) computer password is correct.

When this option is used, and connects to a remote computer, the path’s IP address is populated automatically (see “Send to IP address” on page 144).

7–Path Encryption Settings

Using the path setup menu - Setting up a path on page 129, press [7], and then press [ENTER].

Encryption type

```
P3:Encryption Type:0−None
No:
```

Enter a number to select the following encryption type options:

- Press [0] [ENTER] for none (disabled).
- Press [1] [ENTER] if the Twofish encryption algorithm is required for connection to management software. This option has a 16-character limit on the key length.
- Press [2] [ENTER] if the AES 128-bit encryption algorithm is required for connection to an IP receiver. This option has a 16-character limit on the key length.
- Press [3] [ENTER] if the AES 256-bit encryption algorithm is required for connection to an IP receiver. This option has a 32-character limit on the key length.

Programming the encryption key

The encryption key is programmed as a string of digits, text, a password, or a passphrase. The maximum key length is determined by the encryption type: 16 characters for Twofish or AES 128-bit; or 32 characters for AES 256-bit.

In the following example “Key16” indicates a 16-character limit.

```
P3:Key16:
(1)−Edit
```

To program characters via RAS, see “Programming text via RAS” on page 62.

8–Path Advanced Settings

From the path setup menu - Setting up a path on page 129 - press [8], and then press [ENTER].

Computer attempts

Enter the number of consecutive failed password attempts (in the range 1 to 255) that are permitted before the panel prohibits further attempts. For example, if the number of attempts is set to 3 and the computer has failed to connect 3 times to the Challenger panel, then it will not be able to connect. To re-enable communication you will have to go into this RAS menu option, and then exit.

```
P3:Computer Attempts is 255
No:
```

Enter the number of attempts, and then press [ENTER].

Note: If the number of attempts is set to 0, then the computer will not connect to the Challenger on this path.

Message ACK timeout

Communication formats that are used for reporting events will attempt to connect and then wait for an acknowledgement to be received before making another attempt. The length of time that the panel waits is subject to the path's communication format and the programmed number of retries.

P3:Message ACK Timeout is 1250ms
Time:

The default value for most paths is 0 ms (milliseconds), however, there are other (background) values that determine how long the panel will wait for an acknowledgement to be received. As a result of these background values, you might not need to program a value in the Message ACK Timeout field.

If the path uses format 1 CID Modem, then the length of time that the panel waits for an acknowledgement is a minimum of 1250 ms (this value is compatible with reporting CID via a satellite communications path). If you require a timeout value greater than 1250 ms, then enter the number of milliseconds in the Message ACK Timeout field.

For other applicable communication formats, the length of time that the panel waits for an acknowledgement to be received is comprised of the sum of two values:

- The value of the Message ACK Timeout field, and
- Either 3,000 or 5,000 ms. 3,000 ms is used for the first and second retries; 5,000 ms is used for any further retries.

For example, if the value of the Message ACK Timeout field is 60, and this is the first retry, then the total time that the Challenger panel waits for an acknowledgement to be received is 3,060 ms (3.06 seconds). If you require a timeout value greater than 3,000 or 5,000 ms, then enter the additional number of milliseconds in the Message ACK Timeout field.

Message retries

Message retries is the number of attempts allowed for this path to send an event when the connection is established.

P3:Message Retries is 0
No:

Enter the number of attempts, and then press [ENTER].

Connect timeout

Connect timeout is the length of time in seconds the panel waits before terminating the connection attempt.

```
P3:Connect Timeout is 0s
Time:
```

Enter the number of seconds in the range 1 to 255 (0 means wait indefinitely for a connection), and then press [ENTER].

Connect retries

Connect retries is the number of times this path is to attempt to reconnect after the initial attempt fails.

```
P3:Connect Retries is 0
No:
```

Enter the number of attempts in the range 1 to 255 (0 means that only the initial connection attempt will be made), and then press [ENTER].

Note: If this path is used for IP connection, and a non-zero heartbeat timeout is programmed, then a new connection attempt (if programmed) will be made after the heartbeat timeout expires.

Wait time between connections

Type the number of seconds (1 to 255) that the Challenger panel should wait to retry a connection when events are queued.

```
P3:Wait Time Between Connections is 0s
Time:
```

Enter the time, and then press [ENTER].

Heartbeart timeout

Heartbeat timeout is optionally used for IP or Cellular (3G & 4G) paths to detect a connection failure. When used, the Challenger panel logs an Ethernet Heart Beat fail message to history (and then an Ethernet Heart Beat restore message when reconnected).

Note: The Ethernet heartbeat fail condition is generated only after the path’s programmed number of message retries and connect retries have been exhausted.

```
P3:Heartbeat Timeout is 0s
Time:
```

Enter the time in seconds, and then press [ENTER].

Note: To avoid Ethernet Heart Beat Failed alarms, the Challenger panel’s heartbeat value must be greater than the “heartbeat timeout” value in management software or Tecom IP Receiver.

9–Reset Path Queues

From the path setup menu - Setting up a path on page 129 - press [9], and then press [ENTER].

This option is used to clear this path of stored alarm events, access events, or both access and alarm events that are held in memory. After resetting, only new events will be transmitted.

```
P3:Reset: 1−Alarms (0000) 2−Access (0000) 3−Both
0−Exit, Menu:
```

Press [1] to clear the alarm queue, press [2] to clear the access queue, or [3] to clear both alarm and access queues.

Tip: You can also reset path queues from “Checking communications status” on page 150.

Enter a menu number, and then press [ENTER].

10–Path Authentication

There are two methods for authenticating a connection from a remote computer to a Challenger system:

- Computer password
- Path authentication with user name and password

The default method is computer password, as defined by the path’s **Computer password** option. See “Computer password” on page 134. If a user name and password are defined in these options, then the path’s **Computer password** is ignored, and the remote computer must use the defined user name and password.

From the path setup menu – “Setting up a path” on page 129 – press [10], and then press [ENTER].

Name

Enter a user name for path authentication.

```
P3:Name:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program characters via RAS, see “Programming text via RAS” on page 62.

Password

Enter a password for path authentication.

```
P3:Password:
(1)−Edit
```

The password may contain up to 16 characters (including spaces). To program characters via RAS, see “Programming text via RAS” on page 62.

Checking communications status

The status of each communications sub-system can be quickly displayed via RAS to facilitate installation and troubleshooting.

From the Communications menu - Option 9: Communications, on page 122 - press [3], and then press [ENTER].

```
1−Path Status 2−HW Status 3−MM Software
0−Exit, Menu:
```

Enter a menu number and then press [ENTER]:

- Press [1] [ENTER] for “Path status” below
- Press [2] [ENTER] for “Hardware status” on page 151
- Press [3] [ENTER] for “Management software status” on page 153

Path status

This option enables you to quickly see a summary of the 10 communications paths.

From the status menu (“Checking communications status” above), press [1], and then press [ENTER].

```
Status Comm Path:None
0−Exit, No:
```

Enter a communications path number, and then press [ENTER].

```
Status Comm Path:2−USB INSTALLER *
0−Exit, No:
```

The ‘*’ mark after the name indicates that the displayed path is enabled. Press [ENTER] to see test call status.

```
P2:1−Send Test Call Status: Active
0−Exit:
```

Press [ENTER] to see queue status (example data shown).

```
P2:Queues: Alm:0054 Acc:0147 BU 03
1−3 Reset 0−Exit:
```

The path’s queue status is appended with “BU: nn” when the path is currently in use as a backup for another path (nn) that has lost connection.

Press [1] to clear this path’s alarm queue, press [2] to clear the access queue, or [3] to clear both alarm and access queues.

Note: If this path is currently in use as a backup for another path, clearing this path’s queues does not clear the queues for the path that has lost connection.

Tip: You can also reset path queues from “9–Reset Path Queues” on page 149.

Press [ENTER] to see dialler status (applicable to dialler paths only).

```
P2:Dial Path: None State: NA
0−Exit:
```

Press [ENTER] to see security attempts (example data shown).

```
P2:Security Attempts: 255, Failed 0
1−Reset 0−Exit:
```

Press [1] to reset the count of failed security attempts.

Press [ENTER] to see the state of the path’s connection details (example data shown).

```
P2:YES−Connected YES−Encrypted Ping: Ready
1−Ping 0−Exit:
```

If this path is connected via IP, and the top line displays “Ping: Ready”, you can press [1] [ENTER] to ping the destination IP address. The top line displays “Ping: N/A” if this path is not configured for IP.

After pinging the IP address, the top line displays Ping: and one of the following:

- “Wait…” indicates waiting for response.
- “12ms” (for example) indicates the ping turn-around time in milliseconds (up to 5000 ms).
- “Timeout” indicates there was no ping response within 5000 ms.
- “Error” indicates an attempt to ping a WAN address without a gateway programmed.

Press [ENTER] to see if any paths have the report fail event flag active (example data shown).

```
P2:Report Fail On Paths:03U
0−Exit:
```

The above example indicates that path 3 is in a report fail state. The letter (or letters) following the path name indicates the following conditions:

- “R” means not responding
- “U” means not connected

Note: If you want a path to be able to activate the report fail event flag, the “Trigger Comms Fail Event” option must be enabled in Connection Control.

Press [ENTER] to return to the menu.

Hardware status

From the status menu - Checking communications status on page 150 - press [2], and then press [ENTER].

```
Hardware Status
0−Exit, Menu:
```

Press [ENTER] to see each of the hardware status menu options in turn:

- Press [1] [ENTER] for the onboard Ethernet interface
- Press [2] [ENTER] for a device in expander slot 1
- Press [3] [ENTER] for a device in expander slot 2
- Press [4] [ENTER] for a device in expander slot 3

The first option is described in “Checking the panel’s onboard Ethernet interface” below.

Note: Various devices can be mounted in the panel’s three expander slots, and the programming options vary. Refer to the device’s installation instructions for set up instructions.

Checking the panel’s onboard Ethernet interface

From “Hardware status” on page 151, press [1] [ENTER] to display the status of onboard Ethernet interface (the following examples are based on enabled and connected Ethernet interface).

The first RAS display indicates the condition of the Ethernet interface and link.

In the following examples the Ethernet interface is enabled and the network cable is plugged into a 100 Mbps (or 1Gbps) LAN.

```
Eth: Link Ok (100 Mbps)
Press Enter
```

Other messages indicate the following conditions:

- “Disabled” indicates that the option “Ethernet options

Enable Ethernet” on page 125 is set to No.

- “No Link” indicates that the Ethernet interface is enabled, but the network cable is unplugged.
- “Link Ok (10 Mbps)” indicates that the Ethernet interface is enabled and the network cable is plugged into a 10 Mbps LAN.
- “HW Fail” indicates that an Ethernet interface fault was detected.

Press [ENTER] to display the Ethernet interface’s IP address programmed in “IP address” on page 126:

```
Eth: IP Addr 192.168.000.054
Press Enter
```

Note: If the Ethernet interface does not have a cable connected, the IP address displays 000.000.000.000.

Press [ENTER] to display the Ethernet interface’s MAC address:

```
Eth: MAC Addr 00:17:55:EE:51:01
Press Enter
```

Press [ENTER] to display the number of discarded IP packets:

```
Eth: Pkts Discarded 00000
Press Enter
```

Press [ENTER] to return to the menu.

Management software status

The third option is used if reporting alarms via IP Receiver.

From the status menu - Checking communications status on page 150 - press [3], and then press [ENTER].

```
Enrolled Paths: 1,
1−Enrol 0−Exit
```

If the Challenger panel is configured to communicate with an IP Receiver (via at least one path), select option 1–Enrol to request a connection to IP Receiver.

When the IP Receiver detects communication from a correctly configured Challenger panel on the network at an IP address that is not in its database, it attempts to add the panel to its database by enrolling it.

Press [0] to return to the menu.

UltraSync

Use this option to configure UltraSync communication. For more information about UltraSync and detailed instructions on setting up an UltraSync connection, refer to the “UltraSync Configuration Guide” document.

From the Communications menu - Option 9: Communications, on page 122 - press [4], and then press [ENTER].

```
1−Setup 2−Reports 3−Status 4−Auto Setup
0−Exit, Menu:
```

There are four menu options:

- 1−Setup
- 2−Reports
- 3−Status
- 4−Auto Setup

The options are described in the following sections.

1−Setup

From the UltraSync menu press [1], and then press [ENTER].

Enable UltraSync

```
NO − UltraSync Enabled
*−Change
```

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

Passcode

Passcode: 00000000
Pass:

Enter the UltraSync passcode. This must be changed from the default ‘00000000’ otherwise the UltraSync servers will not accept any connections to or from the panel.

Press [ENTER] to move to the next option.

If UltraSync is enabled, then there are two further menu options that enable you to change the settings for the UltraSync link path (communications path 6 for Ethernet or communications path 7 for radio):

- 1−Alarm filter
- 2−Test calls

1−Alarm filter

The options in this menu reflect the options available in the “3−Path Filter” menu for paths. See “3–Path Filter” on page 137.

2−Test calls

The options in this menu reflect the options available in the “4−Path Test Calls” menu for paths. See “4–Path Test Calls” on page 140.

Press [ENTER] to exit the Setup menu.

2−Reports

From the UltraSync menu press [2], and then press [ENTER].

Enter report number
No:

Enter a report number between 1 and 8.

Press [ENTER] to move to the next option.

Email adresss

1:Addr:
(1)–Edit

Press [1] to change to text edit mode, and use the keypad to enter an email address.

Press [ENTER] to move to the next option.

User

1:User: 0
No:

Enter a user number, and then press [ENTER].

Press [ENTER] to move to the next option.

Alarm events

```
1:NO–Alarm events
*–Change 0–Skip
```

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

Arm/disarm events

```
1:NO–Arm/disarm events
*–Change 0–Skip
```

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

System events

```
1:NO–System events
*–Change 0–Skip
```

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

Power events

```
1:NO–Power events
*–Change 0–Skip
```

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

Trace events

```
1:NO–Trace events
*–Change 0–Skip
```

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to exit the Reports menu.

3−Status

From the UltraSync menu press [3], and then press [ENTER].

The items in this menu show the current status of the UltraSync connection. There are two further menu options:

- 1−Connection status
- 2−Info

1–Connection status

The Connection status menu shows information about the Challenger panel’s connection with UltraSync.

Status summary

The connection status indicates whether the Challenger panel has registered with UltraSync.

```
Status summary: Not configured
0−Exit, No:
```

If UltraSync is set up, then more status options will be displayed.

Press [ENTER] to move to the next option.

Ethernet path

```
Eth. Path: Not configured
0−Exit, *−Refresh
```

If using UltraSync via Ethernet, the Ethernet communications path number will be displayed.

Press [ENTER] to move to the next option.

Ethernet URL

```
Eth. Url1: z65.ultraconnect.com:8081
0−Exit, *−Refresh
```

If using UltraSync via Ethernet, the URL for the UltraSync connection will be displayed.

Press [ENTER] to move to the next option.

Radio path

```
Radio Path: Not configured
0−Exit, *−Refresh
```

If using UltraSync via radio (4G), the radio communications path number will be displayed.

Press [ENTER] to move to the next option.

Radio URL

```
Radio Url1: z65.ultraconnect.com:8081
0−Exit,*−Refresh
```

If using UltraSync via radio (4G), the URL for the UltraSync connection will be displayed.

Press [ENTER] to move to the next option.

Radio location

```
Radio Location: Exp1
0−Exit,*−Refresh
```

If using UltraSync via Cellular (4G), the location (Exp1 or Exp2) of the TS1054 4G Communication Module will be displayed.

Press [ENTER] to exit the Connection status menu.

2–Info

The Info menu shows information about the UltraSync configuration.

Serial number

Shows the Challenger panel’s serial number.

```
Serial No: XXXXXXXXXXXX
0−Exit or Enter
```

If UltraSync is set up, then more information options will be displayed.

Press [ENTER] to move to the next option.

GMT offset

Shows the offset of the Challenger panel in minutes from GMT (Greenwich Mean Time).

```
GMT Offset: +600 mins
0−Exit or Enter
```

Press [ENTER] to move to the next option.

Shows the DST (Daylight Savings Time) start date and time.

```
DST Start: Disabled
0−Exit or Enter
```

Press [ENTER] to move to the next option.

Shows the DST (Daylight Savings Time) end date and time.

```
DST End: Disabled
0−Exit or Enter
```

Press [ENTER] to exit the Info menu.

Press [ENTER] to exit the Status menu.

From the UltraSync menu press [3], and then press [ENTER].

```
Eth. Path: NO
*−Change
```

Press [*] toggle whether to use Ethernet as UltraSync’s link path or not.

Press [ENTER] to move to the next option.

```
Radio Path: NO
*−Change
```

Press [*] toggle whether to use radio (4G) as UltraSync’s link path or not.

Press [ENTER] to move to the next option.

```
Radio Location: Exp1
*−Change
```

If using UltraSync via radio (4G), press [*] to toggle the value of the radio location, which can be either Exp1 or Exp2, depending on where the TS1053 3G Communication Module that will be used for UltraSync is installed.

Press [ENTER] to move to the next option.

```
Run AUTO−SETUP? NO
*−Change
```

Press [*] to run the Auto Setup facility.

The following is displayed on the RAS:

```
AUTO-SETUP BUSY
0−Exit,*−Refresh
```

Press [*] to refresh the Auto Setup status.

If UltraSync connection is successful, then the following is displayed on the RAS:

```
AUTO-SETUP SUCCESS
Press ENTER
```

Press [ENTER] to exit the Auto Setup menu.

Option 10 is not used in this release (formerly Text Words).

Option 11: Version

Firmware version information may be needed when requesting help from technical support.

Select the device for version information

```
Version 1−Chall 2−RAS 3−DGP 4−Exp
0−Exit, Menu:
```

Enter the number for the device type, and then press [ENTER]. In the following example, option 1 is selected.

```
TS-CHPLUS − ChallengerPlus
V10-07.12550
```

Refer to Table 14 on page 159 for details.

Table 14: Device type codes

Number	Device	Information
1	Control panel	Initial display: • Panel model • Firmware revision number Press [ENTER] to display the bootloader version. Press [ENTER] to display the serial number. Press [ENTER] to display the memory type and communications type. Press [ENTER] to display the copyright information.
2	RAS	Type of RAS and version information
3	DGP	Type of DGP, version number, and memory type
4	Exp	See “Displaying expander information” below.

Press [ENTER] to scroll between different information for the same device.

The displayed memory types are:

- “MIUM” indicates 2000 user capacity (Challenger*Plus*)
- “LIUM” indicates 65,535 user capacity (TS1084 module fitted)

The displayed communications types are:

- Full Comms (Challenger*Plus*)

Displaying expander information

If you select option 4–Exp from the Version menu, the following options are listed.

```
Expander 1−Exp1 2−Exp2 3−Exp3
0−Exit, Menu:
```

Enter the number for the expander slot, and then press [ENTER]. The following examples are based on sample data: Expander slots may accommodate more than one type of module.

If a module is not detected in the selected slot, then “Not Present” is displayed.

Expander 1 fitted with a TS1054 4G Communications Interface

```
Exp1: TS1054 − 4G Communication Module
Press ENTER
```

Press [ENTER] to display the module’s firmware revision number.

```
Exp1: Version: V01−02.43147
Press ENTER
```

Press [ENTER] to display the module’s serial number.

```
Exp1: Serial No: 275191780005
Press ENTER
```

Expander 3 fitted with a TS1084 Memory Expansion Module

```
Exp3: TS1084 − Expansion Memory
Press ENTER
```

Press [ENTER] to display the module’s firmware revision number.

```
Exp3: Version: V01−02.45182
Press ENTER
```

Press [ENTER] to display the module’s serial number.

```
Exp3: Serial No:
Press ENTER
```

Press [ENTER] to display the memory type, and database version (assuming that there is a functioning microSD card in place).

```
Exp3: LIUM dbV1.2
Press ENTER
```

If there is a problem with the module’s microSD card, then additional messages display on the top line, as follows:

- “SD CARD NOT INSERTED” indicates that no microSD card was detected in the module’s microSD card port. A microSD card must remain fitted to the module for it to function correctly.
- “EXP HW ERROR” indicates that a hardware fault was detected on the memory expansion module.

Press [ENTER] to exit this option.

Option 12: Lamp test

This option is used to turn on the area, fault, and alarm LEDs in the system’s RASs to verify their operation. It is a RAS-only option (not programmed via management software).

```
Lamp Test is Off
Code:
```

Enter a valid user PIN and then press [ENTER] to activate RAS LEDs.

```
Lamps Active On All Arming Stations
Code:
```

Enter a valid user PIN and then press [ENTER] to return RAS LEDs to their previous states. Press [ENTER] to exit the Lamp Test option.

When finished checking RAS LEDs, ensure that the display shows “OFF” before exiting the option.

Option 13: Time zones

Time zones are used to create time slots in which certain events can take place. Time zones are assigned to alarm groups, door groups, floor groups, relays (outputs), arm and disarm timers, and out-of-hours access reporting, to restrict or enable specific operations during specific time periods.

Time zones (also called ‘hard’ time zones) are numbered 1 to 24 and 42 to 63, and are programmed for specific time periods. Each time zone is made up of one to eight sub-time zones containing:

- A start time
- An end time
- The week days that the sub-time zone is valid
- Up to eight holiday types that the sub-time zone is valid

Use consecutive sub-time zones when a time zone’s start time and end time are on different days. The hours 24:00 and 00:00 are not recognized as end times and can therefore be used to extend a period to the next sub-time zone.

A time zone is invalid on any holiday that has been declared in the holiday date file (user menu 21) unless a corresponding holiday type is included in the sub-time zone. If a holiday type is included, the sub-time zone is valid on defined holiday that have the same type (even if the day of the week that it falls on is not included in the sub-time zone). See “Holiday types” on page 162.

Time zone 0 is a 24-hour time zone (always valid) and is not programmable.

Programming time zones

A worksheet is provided to record programming details and to further describe this option. See “Time zones worksheet” on page 267.

```
Time Zones
Time Zone No:
```

Enter the time zone number, and then press [ENTER] to program a name to identify the time zone.

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Press [ENTER] to display the first of eight sub-time zones (for example TZ 1.1).

```
TZ 1.1 Start − 00:00 End − 00:00
Start Hours:
```

Enter the start time hour, and then press [ENTER].

```
TZ 1.1 Start−08:00 End−00:00
Start Mins:
```

Enter the start time minutes, and then press [ENTER].

```
TZ 1.1 Start−08:30 End−00:00
End Hours:
```

Enter the end time hour, and then press [ENTER].

```
TZ 1.1 Start−08:30 End−1800
End Mins:
```

Enter the end time minutes, and then press [ENTER]. The start and end times programmed will show on the top line of the display.

Press [ENTER] to advance to the day of the week field.

```
TZ 1.1 Days: --,--,--,--,--,--,--,
(1)Sun−(7)Sat:
```

Enter the start day needed, and then press [ENTER]. For the days of the week, enter their numerical value with Sunday as “1” and Saturday as “7”. Repeat for each day needed. The active days will show on the top line of the display.

```
TZ 1.1 Hol Types:
Type (1) − (8)
```

Enter the holiday types needed, and then press [ENTER]. The active holiday types will show on the top line of the display.

When one or more holiday types are selected, the sub-time zone will be valid on holidays that contain the same types.

Note: A sub-time zone is invalid on any defined holiday unless the holiday’s type is included as a day in the sub-time zone.

Holiday types

The Challenger concept of holiday types provides greater flexibility in controlling access for users who need to use the Challenger system during holidays.

Holiday types provide the ability to grant access for users on some holidays and not others. For example:

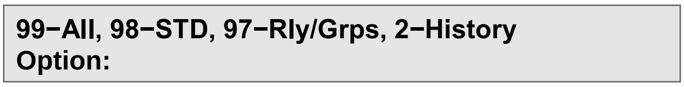
- We want cleaning staff to have access during school holidays, but not on public holidays.
- We want maintenance staff to have access during both school and public holidays.
- School holidays can be designated H1 type, and cleaning staff time zone must contain H1 type.
- Public holidays can be designated H2 type, and maintenance staff time zone must contain H1 and H2 types.

For each holiday type, enter a description of what the type indicates (for example, “School Holidays”) in the Holiday types worksheet, Figure 62 on page 283.

Option 14: Defaults

This option is used to reset the panel to default settings. Defaults is a RAS-only option (not programmed via management software).

The following image displays the first line wrapped over two lines. Some RAS displays would not appear as shown.



```
99−All, 98−STD, 97−Rly/Grps, 2−History
Option:
```

Enter the number for the default type (see Table 15 below), and then press [ENTER].

Table 15: Default options

Number	Action
2	This option deletes all events (messages) in the history and in each communication path’s queue.
97	Resets the relay mapping records, door groups, and floor groups. Relay 2 is defaulted to event flag 2; relay 16 and the 16th relay for each DGP address is defaulted to event flag 1; all other relays are defaulted to no event flag.
98	Defaults the following Install menu options: • Area Database (name and entry/exit times only) • Alarm Groups 11 to 29 • Timers • System Options (except for event text) • Auto Reset • Time Zones • User Categories • Arm/Disarm via time zone • Areas Assigned to Vaults • Area Linking • Time zone to follow relay
99	Defaults all the Install menu options. All programming is erased.
111 This option is not displayed.	Deletes all users (except for the Master Installer) from the Challenger panel or Memory Expansion Module, as applicable.
999 This option is not displayed.	Resets the panel without altering any programming. This option is similar to removing and reapplying power to the system. Can be useful when macros or dialler are not functioning correctly.

Option 15: User category

In Challenger application, user categories 1 to 8 provide timing for an alarm group's areas that are configured for timed disarming or for delayed arming (via vault programming). The user category time is configured in “Option 6: Timers” on page 104.

For user category to function correctly it must be programmed in both the user’s alarm group and in the RAS’s or door’s alarm group.

User category-specific functionality

User category 2 and user category 6 can be used for cleaners or tradespeople to suppress either a local alarm or an event flag from the following input types during access:

- Input type 44 (Access local/secure alarm) disabled by cleaners or trades
- Input type 45 (Access event flag/secure alarm) disabled by cleaners or trades

For example, you might want a fire door to indicate that it’s open during access hours by activating a local alarm (input type 44) or by activating an event flag (input type 45). However, you also might want to inhibit this indication when cleaners and/or tradespeople are working after hours. Refer to Table 28 on page 231 for details.

User category 2 and user category 6 work the same as the others, except that they stop input types 44 and 45 from indicating their unsealed behaviour during access. Both user category 2 and user category 6 categories can be used simultaneously and with different user category times to accommodate users with different needs. For example, cleaners might need to access the area for 15 minutes, and trades might need 60 minutes. In each case, the user would need to enter their code upon entering, even if the area has already been disarmed.

User Category 7 is for security guards who need to check in at intervals. It works the same as the others, except that when the timer expires and the areas rearm, an “emergency” (guard failed to check in) message is reported to the remote monitoring company. The panel reports CID 102 (failed to check in) on point ID 375.

Programming user categories

A worksheet is provided to record programming details and to further describe this option. See “User categories worksheet” on page 268.

User category number

User Category Programming
Cat No:

Enter a number from 1 to 8 for the user category, and then press [ENTER].

User category name

Program a name to identify the user category. The user category name is displayed on an LCD RAS when the user category time is running. If left blank, then " will be displayed on the RAS.

```
1:
(1) −Edit
```

The name may contain up to 30 characters (including spaces).

To program a name via RAS, see “Programming text via RAS” on page 62.

Note: You must program a name in order for management software to retrieve this data.

Option 16: Map relays

This option links a relay (output) to an event flag and/or a time zone. Relays are available as relay cards (TS0840, TS0841, or TS0843) or open collector outputs (TS0842).

An event flag can be active or inactive, and a time zone can be valid or invalid. In addition, the logic has the additional options:

- Active or inactive during time zone
- Non-inverted or inverted

Programming

A worksheet is provided to record programming details and to further describe this option. See “Relay mapping worksheet” on page 269. See also “Programming relays” on page 30.

Relay number

Each relay has a specific number that identifies the relay to the control panel. Relay numbers are assigned according to Table 25 on page 225.

A relay may be mapped to only a single event flag, but the same event flag may be used to indicate multiple conditions (for example, several areas can activate a common siren event flag).

```
Relay Mapping
Relay No:
```

Enter the relay number and then press [ENTER] to program a name to identify the relay.

Relay name

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Press [ENTER] to program an event flag.

Event flag number

An event flag or a time zone activates a relay. If an event flag is nominated (but not a time zone), the relay is active only when the event flag is active.

The relay follows the event flag during a valid time zone. If event flag number 0 is programmed, the relay does not follow any event flag.

Defaults:

- Relay 2 (panel strobe output) is mapped to event flag 2.
- Relay 16 (siren), and the 16th relay for each DGP address, is mapped to event flag 1.

```
Relay 3 Has No Event
Event Flag:
```

Enter the event flag number, and then press [ENTER].

Time zone to control relay

The programmed time zone controls the times that a relay is active (time zone is valid) or inactive (time zone is invalid):

- If the time zone is valid, the state of the event flag is irrelevant.
- If the time zone is invalid, the behaviour is the same as event flag only.
- If no time zone is programmed the output follows only the event flag.
- If a time zone is nominated (but not an event flag), the relay is active only when the time zone is valid.

```
Relay 3 TimeZone Not Programmed
TimeZone No:
```

Enter the time zone number, and then press [ENTER].

Active or inactive during time zone

Select the required behaviour of the relay:

- Active: The relay activates when the time zone is valid regardless of the status of the event flag, provided the relay is not inverted.

- Inactive: The relay does not activate when the time zone is valid regardless of the status of the event flag, provided the relay is not inverted. If the time zone is invalid, the relay follows the event flag.

```
Relay 3 Active During Time Zone
'*' − Change
```

Press [ENTER] - accept the displayed choice. Press [MENU*] - toggle between choices.

Note: If no event flag is programmed, inactive during time zone always results in an inactive relay (unless it is inverted).

Invert relay

Select whether to invert the relay:

- Inverted: Logic controlling the relay is reversed. For example, if active or inactive during time zone determines that the relay is to be ON, this setting would change it to OFF.
- NON-Inverted: The relay follows the logic of the other programming.

```
Relay 3 NON−Inverted
'*' − Change
```

Press [ENTER] - accept the displayed choice. Press [MENU*] - toggle between choices.

Note: The final result (i.e. the relay being active or inactive) depends on whether the logic is non-inverted or inverted.

Relay state

The current state of the relay is displayed.

```
Relay 3 Inactive
Press ENTER
```

Press [ENTER] to exit.

Option 17: Arm/disarm via TZ

Time zones can be used to automatically arm and/or disarm areas.

Each combination of a time zone and an alarm group is called an arm/disarm timer program. There are 16 possible arm/disarm timer programs: a different arm/disarm timer program must be completed for each area or area group, where a different function is required.

The settings in the alarm group (see “Option 5: Alarm groups” on page 96) determine the operation of this function. The function follows the rules of the alarm group regarding alarm control. For example, if the alarm group allows arming and timing, but not disarming, then the areas assigned will only automatically arm.

Programming

A worksheet is provided to record programming details and to further describe this option. See “Arm or disarm via time zone worksheet” on page 270.

Arm/disarm time zone

There are 16 possible arm/disarm timer programs.

```
Arm/Disarm Tz
Program No:
```

Enter the arm/disarm timer program number (1 to 16), and then press [ENTER].

Time zone to arm/disarm

A valid time zone disarms the area.

An invalid or expired time zone expires arms the area.

```
Pgm: 1 TimeZone Not Programmed
TimeZone No:
```

Enter the time zone number to be used for automatic arming/disarming, and then press [ENTER].

Alarm group to auto arm/disarm

The alarm group determines which areas are automatically armed or disarmed and if the specified areas are to be automatically armed, disarmed, or both. If a user category is linked to the alarm group, the automatic arming can be postponed by the user category time.

```
Pgm: 1 Alm−Grp: 14−Area One
Alm−Grp:
```

Enter the alarm group number, and then press [ENTER].

Note: Any alarm group assigned to an arm/disarm timer program must not be programmed with a time zone. The time zone is linked to the alarm group in “Time zone to arm/disarm” above.

Option 18: Vaults

Vault areas are areas that, when armed, will automatically arm other areas after a specified time. Users that have the vault areas (and a user category) in their alarm group can arm the vault areas. The time starts only if all vault areas are armed. Users do not need to have alarm control over the areas that are automatically armed.

By using a special programming procedure, a user category timer starts when all the vault areas are armed. When the timer expires, a non-vault area linked to the vault areas will automatically arm.

For example: A building has three office areas (areas 3, 4, and 5), a common foyer (area 1) and a common cafeteria (area 2). Assigning the office areas as vaults allows the foyer and the cafeteria to be armed at a set time after the last office is armed.

Other programming needed (for this example):

- Use this option to program areas 3, 4, and 5 as vaults. (Because this example is for multiple areas, you will need to create an area group containing areas 3, 4, and 5; and then program the area group as a vault.)
- Set “Disable insert of user category” on page 117 to NO.
- Link the areas to be timed on (1 and 2) to the areas designated as vaults in “Option 19: Area linking” on page 170 (areas 1 and 2 linked to the area group containing areas 3, 4, and 5).
- Program an area group that contains the areas to be automatically armed (1 and 2) so that the areas can be both disarmed and timed. See “Option 36: Area groups” on page 190.
- Program the user category’s time required for delayed arming in “Option 6: Timers” on page 104.
- Program the required alarm groups to activate the user category. See “Option 5: Alarm groups” on page 96.

Programming vault areas

A worksheet is provided to record programming details and to further describe this option. See “Vaults worksheet” on page 271.

```
Vault Area 0
'*'−Grp, Area:
```

If the bottom line displays “‘*’-Grp, Area:”, enter an area number in the range 1 to 99 to assign an area to the vault, and then press [ENTER].

Alternatively, press [*] to assign an area group to the vault.

```
Vault Area Group 0
'*'−Chg, Grp:
```

If the bottom line displays “‘*’-Chg, Grp:”, enter an area group number in the range 1 to 255 to assign an area group to the vault, and then press [ENTER].

Enter the area number, and then press [ENTER].

To remove a programmed area or area group, press [0] [ENTER] when prompted for the area or area group number.

Option 19: Area linking

In a facility with multiple areas, the entrance to the facility is usually shared by all areas. This shared area (common area) should only be armed when the last area is armed. The common area is an additional area that automatically arms as soon as the linked areas are armed.

See “Programming common areas” on page 56 for details.

Programming

A worksheet is provided to record programming details and to further describe this option. See “Area linking worksheet” on page 271.

```
Area Linking
Area:
```

Enter the common area number, and then press [ENTER].

```
Area:1 Linked to Area 0
'*'−Grp, Area:
```

If the bottom line displays “‘*’-Grp, Area:”, enter an area number in the range 1 to 99 to link the area to the common area, and then press [ENTER].

Alternatively, press [*] to link an area group to the common area.

```
Area:1 Linked to Area Group 0
'*'−Chg, Grp:
```

If the bottom line displays “‘*’-Chg, Grp:”, enter an area group number in the range 1 to 255, and then press [ENTER].

To remove a programmed area or area group, press [0] [ENTER] when prompted for the area or area group number.

Option 20: Reserved

Option 20 is not used in this release (formerly Site Code).

Option 21: Input shunts

This option is used to program shunt timers, which control shunt procedures. A shunt procedure inhibits an input from being activated when in an unsealed condition and for a specified interval. For example, a shunt stops a door from generating an alarm when it is opened. If the input is still unsealed after the shunt time expires, the input will generate an alarm, depending on the input type and the status of the area.

A worksheet is provided to record programming details and to further describe this option. See “Input shunt worksheet” on page 272.

Shunt timer number

```
Shunt Timers
Shunt No:
```

Enter the shunt timer number from 1 to 32, and then press [ENTER].

Input number to shunt

The input can be assigned to multiple shunt timers. If the shunt timers have different shunt times, then the shunt time used will be the last one started. The display shows the current input number that relates to this shunt timer.

```
1: Has No Input Assigned
Input No:
```

Enter the input number, and then press [ENTER].

Relay number

The relay condition controls whether or not the input remains shunted. If the relay is active, the input is always shunted. When the relay deactivates, the shunt timer continues to run for the programmed shunt time.

```
1: Has No Relay Assigned
Relay No:
```

Enter the relay number, and then press [ENTER].

Note: The total shunt time is the time the relay activates plus the shunt time.

Shunt time

If the shunt time expires and the input remains unsealed, an alarm condition occurs, depending on the input type. Shunt time values have special rules, as follows:

- Enter a value of 1 to 127 for shunt times of 1 second to 127 seconds.
- Enter a value of 60 for one minute, and 120 for two minutes.
- Do not enter a value of 128. You cannot create a shunt time of 128 seconds.
- Enter a value of (128 + n) for a shunt time of n minutes. For example, if you want a shunt time of 30 minutes, use 128 + 30 to give a value of 158.
- The maximum shunt time that can be programmed is 126 minutes (enter a value of 254).

Note: In Challenger a shunt time of 0 is the same as 1 second.

```
1: Time is Set For (Sec) 0
Shunt Time:
```

Enter the shunt time, and then press [ENTER].

Shunt warning time

The shunt warning time is the time the shunt warning event flag will be activated before the shunt timer expires. If the shunt time is programmed in seconds (a shunt time value of 1 to 127), the warning time is programmed in seconds. If the shunt time is programmed in minutes (a shunt time value of 129 to 254), the warning time is programmed in minutes.

```
1: Shunt Warning is 10
Warn Time:
```

Enter the shunt warning time, and then press [ENTER].

Shunt event flag

The assigned event flag is activated when the shunt timer is running.

```
1: Shunt Event Flag is 0
Event Flag:
```

Enter the event flag number, and then press [ENTER].

Shunt warning event flag

The event flag assigned is activated when the shunt warning time is active.

```
1: Shunt Warning Event Flag is 0
Event Flag:
```

Enter the event flag number, and then press [ENTER].

Shunt RAS

A RAS is assigned in order for the shunt messages to show on the RAS (subject to RAS options) and for the shunt to start from the RAS after the door open command.

```
1: Shunt RAS is 0
RAS Number:
```

Enter the RAS number in the range 1 to 16 or 65 to 80, and then press [ENTER].

Door open command starts shunt

```
1: NO − Door Open Command Start Shunt
*−Change 0−Skip
```

YES A keypad or shunt relay is required to start the shunt timer. If a keypad is used, the user must have a valid door group assigned. The timer resets if the input does not switch to sealed state within either 3 seconds (a shunt time value of 1 to 127) or 3 minutes (a shunt time value of 129 to 254).

NO The condition of the input (sealed to unsealed) triggers the timer.

Note: If this option is set to YES, then “Entry/exit shunting” on page 174 must be set to NO.

Door shunted in access

```
1: NO − Door Shunted In Access
*−Change 0−Skip
```

YES The shunt procedure operates when one or more of the areas assigned to the input are in access.

NO The shunt procedure does not operate when the areas assigned to the input are in access.

Note: At least one of Door Shunted In Access or Door Shunted In Secure must be set to YES for the shunt procedure to operate.

Door shunted in secure

```
1: NO − Door Shunted In Secure
*−Change 0−Skip
```

YES The shunt procedure operates when all of the areas assigned to the input are in secure.

NO The shunt procedure does not operate when the areas assigned to the input are in secure.

Note: At least one of Door Shunted In Access or Door Shunted In Secure must be set to YES for the shunt procedure to operate.

Cancel door event flag

```
1: NO − Cancel Door Event Flag
*−Change 0−Skip
```

YES As soon as the shunted input switches to sealed state, the door unlock event and the shunt timer are cancelled.

NO The door unlock event and the shunt timer are not cancelled if the input switches to sealed.

Input holds event flag at 2 seconds

```
1: NO − Input Holds Event Flag At 2 Sec
*−Change 0−Skip
```

YES In order to allow time for a door to close, there is a 2-second delay after the input switches to sealed state and before it cancels the door event and shunt timer.

NO There is no delay.

Entry/exit shunting

When entry/exit shunting is set to YES, a valid PIN must be entered at the RAS in order to prevent an alarm from being generated. The code may be entered just prior to the door being opened, or before the shunt time expires after the door has been opened.

```
1: NO − Entry/Exit Shunting
*−Change 0−Skip
```

YES A PIN (or access card) is required. The user must have a valid door group assigned and the shunt timer number must be the same as the RAS number.

NO Normal shunt procedure operation.

Note: If this option is set to YES, then “Door open command starts shunt” on page 173 must be set to NO.

Report door open/close

```
1: NO − Report Door Open/Close
*−Change 0−Skip
```

YES Every time the input switches to sealed state and vice versa, it is sent to the printer.

NO Disables the Input status changes being sent to the printer.

Note: If “Print input when unsealed” on page 75 is set to YES for the input assigned to the shunt timer, a door open message is sent twice.

Option 22: Soft time zones

Time zones 26 to 41 are valid only when a relay or output is active. Soft time zones can be used:

- To control doors via a door group. For example, door 17 could be accessed only when a particular relay is active.
- To control alarm groups. If the time zone is assigned to an alarm group, the functions of the alarm group are enabled only when the relay is active.

Examples:

- To prohibit the use of a keypad, unless a key switch on an input is active.
- To allow an area to be disarmed only if another area is disarmed first.

A worksheet is provided to record programming details and to further describe this option. See “Soft time zones worksheet” on page 273. See also “Time zone numbering” on page 228.

Select time zone

```
Relay to TimeZones
TZ (26−41)
```

Enter a time zone number in the range 26 to 41, and then press [ENTER] to program a name to identify the soft time zone.

```
00026:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Assign relay to time zone

```
Tz 27 To Follow Relay 3
Relay No:
```

Enter the relay or output number that the time zone must follow, and then press [ENTER].

Option 23: Poll errors

Use this option to view the number of errors detected in communications between the control panel and the devices connected to the control panel.

Select device type

```
1−RAS, 2−DGP, 3−Clear, 4−DC counters
0−Exit, Menu:
```

Enter the number for the device type (see Table 16 below), and then press [ENTER]. The count for the first device of the selected type displays.

```
RAS 1, Poll Error Count is 0
0−Exit, RAS No:
```

Enter the number for the next device, and then press [ENTER]. Alternatively, press [*] to step though the devices in sequence. Press [ENTER] when finished.

Note: Reset all poll error counters when the system is error-free after installation. If you do not, errors that occurred during installation could distort future error count. The maximum error count that can be recorded is 255.

Table 16: Device type codes

Number	Device	Description
1	RAS	View poll errors for remote arming stations.
2	DGP	View poll errors for data gathering panels.
3	all	Reset all poll error counters.
4	Intelligent Access Controller	View the counts for: • Users sent to each door/lift controller via menu option 24 Send Programming. • Acknowledgements from the door/lift controller (should match the users sent). • “Card not in IUM” messages that caused the panel to send a known user. If the user is known in the panel, but not in the door/lift controller, this count will be incremented by one.

Option 24: Send Programming

Use this option to send access control data for Intelligent Access Controllers (4-door or 4-lift DGPs) that may not have been sent automatically.

Changes to data for Intelligent Access Controllers that are polled and are online are normally sent automatically. However, if a controller is added to the system at a later date or has been defaulted then you can use this option to send the data to the controller. Storing this data in both the control panel and the Intelligent Access Controller enables the controller to provide access control functionality even if it loses communications with the control panel.

```
1−Display Status 2−Send All
Option:
```

Send options

From the Send Programming menu, enter [2], and then press [ENTER] to display the send options.

```
1−Kill 2−Users 3−Grps 4−Tz 5−Hol
Option:
```

Enter a send option number (see Table 17 below), and then press [ENTER] to perform the corresponding action and return to the Send Programming menu screen.

Table 17: Send action codes

Number	Description
1	Kill any sending operation in progress and erase from the Intelligent Access Controller the current database being sent.
2	Send all users.
3	Send door groups and floor groups.
4	Send time zones 0 to 24 and 42 to 63.
5	Send holidays.

Send status

From the Send Programming menu, enter [1], and then press [ENTER] to display the status of the current send operation. For example, if you are sending the user database, the screen may resemble the following.

```
Add User 3444 − 11466
Queue = 0200
```

Press [NEXT *] to update the LCD screen and see the latest status. The display includes:

- The database being sent.
- The number of records already sent.
- The total number of records possible for this option.
- The number of records queued (remaining) to be sent.

Option 25: Display last card

Use this option to show the RAS number and card data of the last card read by a reader connected directly to the control panel (for doors 1 to 16 on LAN 1 and doors 65 to 80 on LAN 2).

This option displays the RAS number, card data format, and raw card data, as shown below.

```
Last Card RAS−1 27.0.0.7.255.1.0
Press ENTER
```

The sample display shows the card data format as 27-bit and the user's raw card data as 0.0.7.255.1.0.

Press [ENTER] to exit the menu.

Option 26: Diagnostics

Option 26 is reserved for factory use to assist with testing and troubleshooting. This menu should be avoided unless specifically instructed by Interlogix tech support.

Option 27: Reserved

Option 27 is not used in this release (formerly Tecom Address mapping).

Option 28: Remote controllers

Use this option to access additional programming menus for remote devices such as a RAS, an Intelligent Access Controller DGP, or a TS0862 Smart Door Controller (which is addressed and polled as a RAS).

Note: The remote device must be:

- Connected to the system LAN.
- Addressed as a RAS or DGP.
- Programmed to be polled in "Poll RAS" on page 84 or "Poll DGP" on page 93.
- If a DGP, it must be programmed with the correct type.
- If a RAS, it must have an onboard programming menu (selected models only).

Select the device type

```
Remote Type: 1−DGP, 2−RAS
Type No:
```

Enter 1 to select a DGP or enter 2 to select a RAS, and then press [ENTER].

Note: Older RAS models do not have an onboard programming menu.

Select the device to program

```
Remote XXX Set−Up
XXX No:
```

Enter the device number (the RAS’s or DGP’s address), and then press [ENTER].

```
"#"−Move On, "*"−Move Back
Menu:
```

Press [ENTER] (#) to continue device programming.

Note: For further information on programming the remote device, see the programming manual for the device selected.

Option 29: Panel voltage & current

This option displays the panel’s supply voltage (V), current draw in amperes (A), and the current supplied to the battery (or from the battery if negative) in amperes (A).

```
Panel: 13.64V, 0.44A Battery: 0.09A
(*)Next or ENTER
```

Press [NEXT] to update the display. Press [ENTER] to exit.

Option 30: Reserved

Option 30 is not used in this release (formerly Printer).

Option 31: Battery testing

Use this option to program automatic battery testing or to perform manual battery testing.

Note: Battery testing is not enabled as a default setting.

During the battery test, the control panel, DGPs, and all auxiliary driven devices, are powered from the battery. Devices are tested starting at 10 second intervals, ensuring that all devices do not switch to battery test at the same time.

A worksheet is provided to record programming details and to further describe this option. See “Battery testing worksheet” on page 273.

Select battery test program

```
Battery Testing 1−Program, 2−Test
0−Skip, Menu:
```

Enter 1 to program the battery test options, or enter 2 to perform a manual battery test, and then press [ENTER].

If you enter 1 (Program), you will see “Battery test frequency” below. If you enter 2 (Test), you will see “Manual battery test” on page 181.

Battery test frequency

This option displays for a programmed battery test.

```
Batt Test Frequency − Every Monday
*−Change 0−Skip
```

To specify how often the automatic battery test should be performed, press [MENU*] to scroll through the options below until the display shows the correct option, then press [ENTER].

Options:

- Disabled
- Every working day
- Every Monday
- First Monday of month

Note: If an instance of a scheduled battery test falls on a programmed holiday, that instance will not run.

Start battery test

This option displays for a programmed battery test.

```
Start Battery Test: 10:00
Hours:
```

Enter the time of day, in hours and minutes, when the battery test will start, and then press [ENTER].

Battery test period

This option displays for a programmed battery test.

```
Run Battery Test For 001
Minutes:
```

Enter the period, in minutes, that the automatic battery test will run, and then press [ENTER]. If a battery test on any device fails, that device immediately restores mains power.

When you press [ENTER] you will exit the menu.

Manual battery test

This option displays for option 2 (Test), in “Select battery test program” on page 180.

```
No DGP Battery Testing in Progress
ENTER
```

This test allows the control panel and DGP batteries to be tested manually. This test does not affect the automatic battery test. The numbers of any DGPs currently in test are displayed.

Press [ENTER] to move to the next manual battery test display.

Battery test report

This option displays for option 2 (Test), in “Select battery test program” on page 180.

```
All DGP Battery Tested OK
ENTER
```

The display shows the results of the previous manual battery test. Press [*] to see additional DGP results (if any).

Press [ENTER] to move to the next manual battery test display.

Select DGP number for battery test

```
Manual Battery Test For DGP # 1−32
DGP:
```

Enter the DGP number in the range 1 to 15 or 17 to 32 for a DGP, or enter 16 for the control panel, and then press [ENTER].

If a DGP number is entered for a unit that does not have a battery, the display will show “Invalid Command for DGP Type”.

Press [ENTER] to exit Battery Testing.

Manual battery test period

```
Run Battery Test For 001
Minutes:
```

Enter the period, in minutes, that the manual battery test will run, and then press [ENTER].

Option 32: Custom message

A worksheet is provided to record programming details and to further describe this option. See “Custom message worksheet” on page 274.

This option creates a customised text message for the top line of the RAS’s initial LCD screen. The text message can include numbers, spaces, and punctuation marks.

(1)−Edit

Use the text option on the keypad to enter a text message of up to 32 characters (see Table 5 on page 62). Use the number keys to enter the required letters from left to right.

To use the panel’s time and date as the custom message, use the number keys to enter a period (.) as the first and only character in the message. The time and date will be displayed in the following format:

HH:MM Day/Month/Year (example: 11:45 26/06/2013)

Option 33: Program next service

This option programs when the next routine service call is due and the display message. The user will be prompted with this programmable message on the LCD to call the installer.

A worksheet is provided to record programming details and to further describe this option. See “Next service date worksheet” on page 274.

Maintenance date

Enter the date when the user will receive the next message prompt that maintenance is due.

Service Required at 0/0/0
Enter Day:

Enter the day of the month and press [ENTER] [ENTER].

Enter the month and press [ENTER] [ENTER].

Enter the year and press [ENTER] [ENTER].

Maintenance message

Use the text option on the keypad to enter a message to display when service is due.

(1)−Edit

The message may contain up to 32 characters (including spaces). To program text via RAS, see “Programming text via RAS” on page 62.

Option 34: Program summary event flags

Summary event flags are triggered on system-wide events such as mains failures or DGPs going offline.

For example, to detect mains fail:

- Activate the mains fail summary event flag.
- Trigger a relay in response to the event flag.

The system alarm or fault event flags will be latching if latching system alarms is set to YES (see “System alarms” on page 117).

Note: User defined event flags are numbered 17 to 255.

To program the following summary event flags options:

1. Choose an unused event flag number.
2. Decide what relay the event flag will activate and under what times and conditions.
3. In “Option 16: Map relays” on page 165 map the event flag to the required relay.
4. Record the event flag details on an event flag worksheet.

Refer to “Event flags” on page 242 for details of these and other types of event flags. A worksheet is provided to record programming details and to further describe this option. See “Event flags worksheets” on page 274.

Mains fail event flag

This event flag is activated when a mains failure is detected on the control panel or on a DGP.

Mains Fail No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Low battery event flag

This event flag is activated when a low battery is detected on the control panel or on a DGP.

Low Battery No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Fuse fail event flag

This event flag is activated when a fuse failure is detected on the control panel or on a DGP.

Fuse Fail No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Tamper event flag

This event flag is activated when a panel tamper is detected on the control panel or on a DGP.

Tamper No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Siren fail event flag

This event flag is activated when a siren fail condition is detected on the control panel or on a DGP.

Siren Fail No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

DGP isolate event flag

This event flag is activated when a DGP has been isolated.

DGP Isolate No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

DGP offline event flag

This event flag is activated when a DGP programmed to be polled does not respond to polling.

```
DGP Offline No Event Flag
Event Flag:
```

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

RAS offline event flag

This event flag is activated when a RAS programmed to be polled does not respond to polling.

```
RAS Offline No Event Flag
Event Flag:
```

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Duress event flag

This event flag is activated when a keypad duress alarm occurs.

```
Duress No Event Flag
Event Flag:
```

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Film out event flag

This event flag is activated when the film count for a camera exceeds the film out level (see “Film out” on page 110).

```
Film Out No Event Flag
Event Flag:
```

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Report fail event flag

This event flag is activated for paths that have Trigger Comms Fail Event enabled to indicate, for example, that the control panel failed to report to the remote monitoring company on the first (and second, if applicable) phone numbers following the number of redial attempts programmed in “Number of redials” on page 142.

Report Fail No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Test mode event flag

This event flag is activated when the control panel is in test mode.

Testmode No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

All secured event flag

This event flag is activated when all areas have been armed, there are no alarm conditions, and no entry/exit timers running.

All Secured No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Console trigger event flag

When this event flag is activated, all RAS buzzers are activated. The event flag also has to be assigned to the events that the RAS buzzer sounds on.

Console Trigger No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Area search running event flag

The event flag specified here is activated when an area search is active. See “Using Area Search” on page 56.

Area Search Running No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Area search done event flag

The event flag specified here is activated when an area search ends, and is deactivated with the area search time zone becomes invalid. See “Using Area Search” on page 56.

Area Search Done No Event Flag
Event Flag:

Enter an unused event flag number, and then press [ENTER]. Enter 0 to disable an event flag.

Option 35: Program macro logic

A macro logic equation is a tool for activating inputs or event flags based on the conditions of one to four macro inputs (event flags or relays).

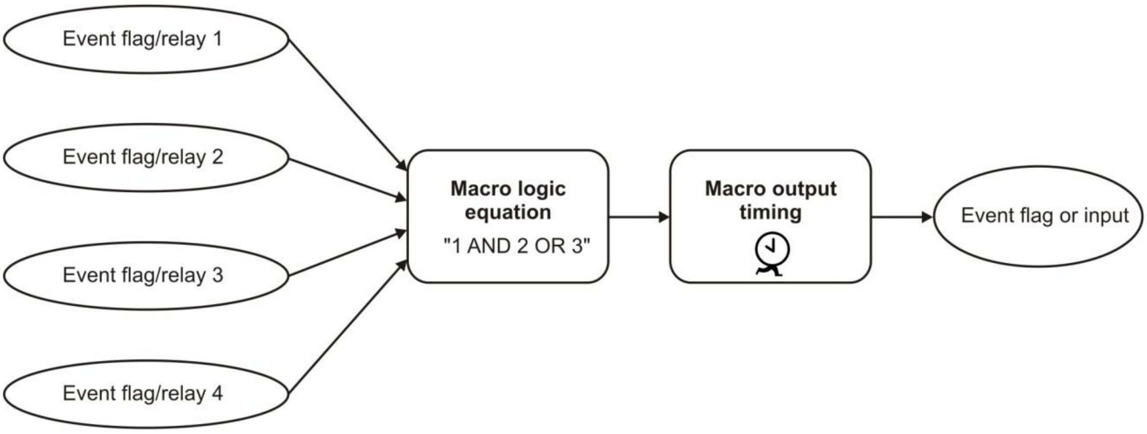
The macro logic equation can combine macro inputs using AND or OR logic, based on the event flag’s or relay’s active or inactive (inverted) state.

The output of the macro logic equation is an event flag or input. “NAND” and “NOR” functions can be made by inverting the logic of the particular input.

Programming options are provided so that the macro result will trigger a macro input as a pulse, time, on delay, off delay, or latch, when activated (see Table 18 on page 188).

When the latched function is used, the fourth macro input resets the output and does not use the AND/OR selections.

Figure 26: Overview of macro logic



Note: It is very important to plan the macro logic carefully, noting all details and the origin of every input and event flag, before attempting to program.

A worksheet is provided to record programming details and to further describe this option. See “Macro logic worksheet” on page 277. See also “Programming macros” on page 48.

Macro number

```
Macro Logic
No:
```

Enter the number of the macro logic program in the range 1 to 48, and then press [ENTER] to program a name.

Macro name

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Macro output function

```
M 1 Disabled
*−Chg, 0−Exit
```

Press [MENU*] to scroll through the function options listed in Table 18 below.

Press [ENTER] to accept the displayed option, or enter 0 to exit menu.

See also “Examples of macro function selections” on page 49.

Table 18: Macro output options

Option	Function
Disabled	This macro logic program is disabled.
Nontimed	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.
On pulse	Activates for the programmed time or the active period of the logic result, whichever is shortest.
On timed	Activates for the programmed time regardless of the macro output changing.
On delay	Activates after the programmed time unless the result of the logic equation is no longer valid.
Off delay	Follows the result of the logic equation, but remains active for the time programmed after the result of the logic equation is no longer active.
Latched	Activities on any of the first three macro inputs in the logic equation and is only reset by the fourth macro input. Any programmed AND / OR function is not used.

Time

```
M1 Times for 0 Seconds
Time:
```

Enter the time period (1 to 255 seconds or minutes) that is used when any of the timed macro output functions are selected (pulse, on timed, on delay, or off delay), and then press [ENTER].

Macro output triggers event flag or input

```
M1 Activates Event Flag 0
*−Chg, No:
```

Specify whether the macro output should trigger an event flag or an input, and then specify which event flag or input.

Press [MENU*] to toggle between “Event Flag” and “Input”.

Enter the event flag or input number and press [ENTER] to display the event flag or input to be programmed.

Enter the same number twice to invert the macro output. It will now trigger the event flag or output if the result of the equation is not true. An inverted macro output is indicated by the exclamation mark (!) preceding the number.

When the display shows the correct number, press [ENTER] to save the display and move to the next option.

Macro inputs

```
M 1 = E0 Or E0 Or E0 Or E0
*−Chg, Input 1:
```

Program up to four macro inputs (event flag or relay numbers).

When all conditions of the logic equation are met, the macro output is active and the event flag or input programmed in the previous step is activated (depending on any timing function programmed on the macro output).

Press [MENU*] to toggle between “E” (event flag) and “R” (relay).

Enter the event flag or relay number and press [ENTER] to display the event flag or relay to be programmed.

Enter the same number twice to invert the macro input. An inverted macro input is identified by the exclamation mark (!) preceding the “E” or “R”.

When the display shows the correct number, press [ENTER] to save the display and move to the next option.

Macro logic equation

```
M 1 = E0 Or E0 Or E0 Or E0
*−Chg, Logic 1:
```

Specify the logical operators that create the macro logic equation. Two operators are available, as follows:

- AND — Result is true only if both inputs are active.
- OR — Result is true if one of the inputs is active.

Press [MENU*] to toggle between AND or OR.

Press [ENTER] to save the displayed information and to return to the original macro logic display.

Note: NAND and NOR functions can be made by inverting the logic of the particular input. Any unused macro inputs must be left as an “OR”.

Option 36: Area groups

A Challenger system can have 99 areas. To help manage areas, one or more areas can be incorporated into area groups. There can be 255 area groups.

Note: Area Group 1 contains all areas by default. If the Challenger panel does not need all areas, we recommend removing unneeded areas from Area Group 1.

Each area in an area group must be configured to allow certain users (as specified by the user’s alarm group) to have permissions for arming, disarming, alarm reset, and for timing.

Create a new area group to provide customized control over each area's permissions for arming, disarming, alarm reset, and for timing.

```
Area Groups
Group No:
```

Enter an area group number from 1 to 255, and then press [ENTER] to program a name.

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

```
Area Grp 2:
Area No:
```

To add the first area to the group, enter an area number in the range 1 to 99, and then press [ENTER] to program the permissions for the area.

The first line indicates the item being programmed. For example, “G2A1” means “Area Group 2, Area 1”.

```
G2A1:NO−Enable
*−Change 0−Skip
```

If required, press [*] to enable this area in the group, and then press [ENTER].

```
G2A1:NO−Arming
*−Change 0−Skip
```

If required, press [*] to allow this area to be armed, and then press [ENTER].

```
G2A1:NO−Disarm
*−Change 0−Skip
```

If required, press [*] to allow this area to be disarmed, and then press [ENTER].

```
G2A1:NO−Reset
*−Change 0−Skip
```

If required, press [*] to allow alarms in this area to be reset, and then press [ENTER].

```
G2A1:NO−Time
*−Change 0−Skip
```

If required, press [*] to allow this area to be time disarmed, and then press [ENTER]. The permission for disarming must also be enabled.

Note: After you add the first area to the group and scroll through the options, you can continue adding areas by enabling them as you come to them, or by returning to the area group later and adding the next area by number.

Option 37: SD card backup/restore

Challenger panels have an onboard SD card port (J20) that can be used by installers to:

- Backup a Challenger panel’s programming to an SD card.
- Restore a Challenger panel’s programming from a previously-saved backup on an SD card.

The SD card can be left in the SD card port permanently so that it can be used for periodic backups, or it can be removed for offsite storage.

Notes

- Records for RASs and DGPs can be backed up only if the devices are currently being polled (as is the case with retrieving to management software).
- Backup files are named “CONFIG.SDR”. Performing a backup overwrites any previous backup on the SD card.
- If you remove a SD card containing a backup file from the panel, you must take appropriate measures to prevent unauthorised use.

This functionality may be used where the Challenger panel is not connected to management software for backup purposes, or to use a Challenger panel’s programming as a template to quickly and consistently configure new panels.

```
1−Backup To SD, 2−Restore From SD, 3−Status
Option:
```

Enter a number to select the following encryption type options:

- Press [1] [ENTER] to back up the Challenger panel’s programming to the SD card in the SD port.
- Press [2] [ENTER] to restore Challenger panel’s programming from a previously-saved backup.
- Press [3] [ENTER] to check the state of a backup or restore command.

Backup to SD Card

When you select option 1 Backup To SD (and there is an SD card in the SD port) the following Status message displays.

```
Status: Backing up, in progress
0−Exit, *−Refresh
```

Press * to update the Status message.

The following messages may be displayed:

- “Idle, no SD card found” means that the panel could not detect the SD card.
- “Idle, couldn’t open file” means that the SD card or the backup file is locked.
- “Idle, write to file failed” means that there is insufficient space on the SD card.

Restore from SD Card

When you select option 2 Restore From SD (and there is a backup file named “CONFIG.SDR” on the SD card) the following Status message displays.

```
Status: Verifying configuration, in progress
0−Exit, *−Refresh
```

Press * to update the Status message.

The following messages may be displayed:

- “Idle, no SD card found” means that the panel could not detect the SD card.
- “Idle, couldn’t open file” means that there is no backup file.

When complete, areas 1 to 16 will be armed and the RAS returns to the default welcome screen.

Note: Restoring a large database with thousands of users can take several minutes.

Option 38: Reset input test days

After programming timed input testing (see “Using timed input testing” on page 61) you may need to reset the input timer before handing the system over to the customer.

```
Reset test days '1' to Reset
Enter to Exit:
```

Press [1] to restart the test days time, and then press [ENTER].

Option 39: Automation

Use the Automation menu to configure automation zones.

An automation zone is one or more building devices (including C-Bus® devices) that can be controlled via the Challenger panel.

The automation zone record enables control to (and optionally feedback from) one or more devices in a C-Bus group. This section refers to such devices as an ‘automation zone’ even if it applies to a C-Bus group.

Refer to “Controlling automation zones via RAS” on page 63 for details about manually turning automation zones on and off via an LCD RAS.

A worksheet is provided to record programming details and to further describe this option. See “Automation zones worksheet” on page 284.

Automation zone number

```
Automation Zone Programming
Enter Zone:
```

Enter an automation zone number in the range 1 to 100, and then press [ENTER].

Name

Program a name to identify the automation zone.

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Enable zone

When the automation zone is enabled, the Challenger panel can interact with it.

```
1:NO − Enable Zone
*−Change
```

Change the value if needed, or press [ENTER] to move to the next option.

Event flag to trigger zone

An event flag is used to trigger the automation zone.

```
Event Flag to Trigger Zone is 0
E/F No:
```

Enter the event flag number, and then press [ENTER].

Invert trigger

This option can trigger the automation zone when the nominated event flag is inactive.

```
1:NO − Invert Trigger
*−Change
```

Change the value if needed, or press [ENTER] to move to the next option.

Time zone to disable trigger

Nominate a hard or soft time zone in which the event flag cannot trigger the automation zone.

```
1: TZ to Disable Trigger is 0
Enter Tz
```

Enter the time zone number in the range 0 to 63, and then press [ENTER].

Time zone to trigger zone

Nominate a hard or soft time zone to trigger the automation zone (regardless of an event flag).

```
1: TZ to Trigger Zone is 0
Enter Tz
```

Enter the time zone number in the range 0 to 63, and then press [ENTER].

When zone triggered set level to

This option determines the automation zone’s maximum value (such as the brightness of lights) when triggered (turned on) by the Challenger panel.

```
1: When Zone Triggered set level to OFF
Level%:
```

Enter a value in the range 0 (off) to 100 (on), and then press [ENTER].

When zone reset set level to

This option determines the automation zone’s minimum value (such as the brightness of lights) when reset (turned off) by the Challenger panel.

```
1: When Zone Reset set level to OFF
Level%:
```

Enter a value in the range 0 (off) to 100 (on), and then press [ENTER].

When triggered zone on for

This option determines the duration in seconds that the automation zone will be at maximum value (including ramp time) when triggered by the Challenger panel.

```
1: When Triggered Zone on for 0 Sec
Enter Sec:
```

Enter a value in the range 0 (not timed) to 65,535 seconds, and then press [ENTER].

Ramp rate

This option determines the rate (speed) of change when the automation zone changes between on and off values.

```
1: Ramp Rate 0−Instant
Opt No:
```

Enter a number to select the following ramp options:

- Press [0] [ENTER] for instant changes.
- Press [1] [ENTER] for change over 4 seconds.
- Press [2] [ENTER] for change over 8 seconds.
- Press [3] [ENTER] for change over 12 seconds.
- Press [4] [ENTER] for change over 20 seconds.
- Press [5] [ENTER] for change over 30 seconds.
- Press [6] [ENTER] for change over 40 seconds.
- Press [7] [ENTER] for change over 60 seconds.
- Press [8] [ENTER] for change over 90 seconds.
- Press [9] [ENTER] for change over 2 minutes.
- Press [10] [ENTER] for change over 3 minutes.
- Press [11] [ENTER] for change over 5 minutes.
- Press [12] [ENTER] for change over 7 minutes.
- Press [13] [ENTER] for change over 10 minutes.
- Press [14] [ENTER] for change over 15 minutes.

- Press [15] [ENTER] for change over 17 minutes.

Press [ENTER] to move to the next option.

Enable logging

Use this option to log the automation zone’s C-Bus events to the panel’s history.

```
1:NO − Enable Logging
*−Change
```

Change the value if needed, or press [ENTER] to move to the next option.

Enable quick control

Use this option to enable quick control via supported RAS models.

```
1:NO − Enable Quick Control
*−Change
```

Change the value if needed, or press [ENTER] to move to the next option.

Note: Quick control does not require user authentication via PIN. We recommend that control be assigned to a specific RAS (in a secure area) in “Control zone on RAS” on page 197 in order to prevent unauthorised use.

Enable manual control

Use this option to enable control via User menu 24–Automation Control and to allow users to activate (trigger) the automation zone (installers can manually activate the automation zone via Install menu option 43–Automation Status without this option being enabled).

```
1:NO − Enable Manual Control
*−Change
```

Change the value if needed, or press [ENTER] to move to the next option.

Manual on control

Use this option to enable installers and users to turn the automation zone on immediately at 100% until turned off or triggered (in which case the zone’s programming will turn it off).

```
1:NO − Manual On Control
*−Change
```

Change the value if needed, or press [ENTER] to move to the next option.

Manual off control

Use this option to enable installers and users to turn the automation zone off (reset) immediately.

```
1:NO − Manual Off Control
*−Change
```

Change the value if needed, or press [ENTER] to move to the next option.

Control zone on RAS

Use this option to specify which LCD RASs can be used to control the automation zone from User menu 24 Automation Control or via quick control.

```
1:Control Zone on RAS 1
0−All RAS No:
```

Enter a value in the range 0 (all RASs) or a single RAS at address 1 to 16 or 65 to 80, and then press [ENTER] to move to the next option.

Notes:

- Automation zones can be controlled from any LCD RAS via Install menu “Option 43: Automation status” on page 200.
- Quick control does not require user authentication via PIN. We recommend that control be assigned to a specific RAS (in a secure area) in order to prevent unauthorised use.

Zone activates event flag

This option applies only to the “C-Bus with Feedback” zone type.

You can program a Challenger event flag to be activated when the automation zone is activated.

```
1: Zone Activates Event Flag 0
E/F no:
```

Enter the event flag number, and then press [ENTER].

Set event flag at level

This option applies only to the “C-Bus with Feedback” zone type.

When the automation zone reaches a specified dimming level, the associated Challenger event flag is set (activated). For example, set the event flag when the automation zone reaches 90% brightness.

```
1: Set Event Flag at Level OFF
Level%:
```

Enter a value in the range 0 (off) to 100 (on), and then press [ENTER].

Reset event flag at level

This option applies only to the “C-Bus with Feedback” zone type.

When the C-Bus zone reaches a specified dimming level, the associated Challenger event flag is reset (deactivated). For example, reset the event flag when the automation zone reaches 30% brightness.

```
1: Reset Event Flag at Level OFF
Level%:
```

Enter a value in the range 0 (off) to 100 (on), and then press [ENTER].

Zone type

This option determines the behaviour of the automation zone.

```
1: Type 0−Internal
Opt No:
```

Enter a number to select the following type options:

- Press [0] [ENTER] for internal (reserved).
- Press [1] [ENTER] for Tecom (reserved).
- Press [2] [ENTER] for Tecom with feedback (reserved).
- Press [3] [ENTER] for C-Bus.
- Press [4] [ENTER] for C-Bus with Feedback.

Press [ENTER] to move to the next option.

Group number

This option applies to the “C-Bus” and “C-Bus with Feedback” zone types.

Group number associates this automation zone record with a C-Bus group for monitoring and controlling.

```
1: This zone is set to Group 0
Group no:
```

Enter a number in the range 0 to 255, and then press [ENTER] to move to the next option.

Network Number

This option applies to the “C-Bus” and “C-Bus with Feedback” zone types.

Network number tells the Challenger panel what C-Bus network the zone uses.

```
1: This zone is set to Network 0
Network no:
```

Enter a number in the range 0 to 255, and then press [ENTER] to move to the next option. This value is typically set to 0 if a C-bus network bridge is not used.

App Number

This option applies to the “C-Bus” and “C-Bus with Feedback” zone types.

The devices in the C-Bus group may be filtered via C-Bus application address designations. If applicable, enter the C-Bus application address.

```
1: This zone is set to App 0
App no:
```

Enter a number in the range 0 to 255, and then press [ENTER] to exit from this automation zone’s programming.

Option 40: Door/lift names and E/F trigger

Challenger panels can control 128 doors (32 doors via RASs and 96 doors via Four-Door Controllers) or 96 lifts (via Four-Lift Controllers).

Use Door & Lift Setup to configure a door’s or lift’s name, event flag and event flag trigger duration (typically for use as an automation zone trigger).

Door or lift number

```
Door & Lift setup
No:
```

Enter a number in the range 1 to 128, and then press [ENTER].

Name

Program a name to identify the door or lift.

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Note: The Door name is the same as the (same numbered) RAS name, programmed in “Option 3: RAS database” on page 83.

Event flag

You can program an event flag to be activated when the door is unlocked or the lift is accessed, and you can program a time for the event flag to be activated.

In the case of RAS doors, the event flag is an alternative to a RAS's 'door event flag', which is activated for the door unlock time programmed in Timers.

```
1: E/F to Trigger 0
E/F No:
```

Time to trigger

Program the time for the event flag to be activated:

```
1: Time to Trigger for 00000
Time (Sec):
```

Enter the number of seconds from 0 to 65,535 (0 is not timed), and then press [ENTER].

Option 41: Event flag names

A Challenger panel's event flags can be assigned names. Use this option to assign or change an event flag's name.

```
Select Event Flag
EF No:
```

Enter the event flag number in the range 1 to 255, and then press [ENTER].

```
1:
(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see "Programming text via RAS" on page 62.

Option 42: Challenger name

You can enter a name to describe the Challenger panel.

```

(1)−Edit
```

The name may contain up to 30 characters (including spaces). To program a name via RAS, see "Programming text via RAS" on page 62.

Option 43: Automation status

Use this option to control automation zones via from any LCD RAS.

```
Automation Zone
0−Exit, Zone:
```

Enter the number of the zone, and then press [ENTER] to move to the next option.

```
1: Entrance lights − OFF
1−Trig 2−On 3−Off
```

The top line indicates the current state of the zone. Press a number to perform the following actions:

- Press [1] to trigger the automation zone according to its programming.
- Press [2] to turn the automation zone on immediately at 100% until turned off or triggered (in which case the zone’s programming will turn it off). This option is displayed only if “Manual on control” on page 196 is enabled.
- Press [3] to turn the zone off (reset) the zone. This option is displayed only if “Manual off control” on page 197 is enabled.

Press [ENTER] to move to the next higher automation zone number, or to exit if there are no higher zone numbers.

Option 44: Standard lifts

ChallengerPlus panels can support two lifts with up to ten floors each, without requiring a Four-Lift Controller.

Each lift may have up to two reader interfaces:

- The **local reader** is the standard lift reader where a user can badge a card or enter a PIN to activate their desired floor.
- The **remote reader** enables the user to remotely activate the floor to allow a visitor to access the lift and select the desired floor.

Each reader has an access timer. This allows the remote reader to be configured with an extended access time compared to the local reader. For example, the remote reader can be configured with enough time for a visitor to cross an apartment building’s foyer to get to the lift and select the desired floor.

An override floor group can be configured for each lift so that certain floors can be accessed at certain times of the day, without requiring a valid card or PIN at the lift reader.

A security event flag and security floor group can be configured for each lift. When the security event flag is activated, the security floor group is activated. The security floor group allows certain floors to be accessed at certain times of the day, without requiring a valid card or PIN at the lift reader, provided the security event flag is activated.

The time that a floor will be active for will be determined based on which reader has activated it. For example, if a floor relay has been activated via a remote reader, and another floor relay has been activated by the local reader, then each floor relay will be active for the appropriate amount of time. This allows multiple remote readers to activate multiple floor relays.

See the *ChallengerPlus Administrators Manual* for more information on programming floor groups.

A worksheet is provided to record programming details and to further describe this option. See “Standard lifts worksheet” on page 286.

Lift number

```
Enter lift number to add/edit
Lift No:
```

Enter a number in the range 1 to 126, and then press [ENTER].

Create lift

If the lift does not exist, the RAS will prompt you to create it.

```
1:Create lift
0−Exit 1−Create
```

A maximum of two lifts can be created.

Press [1] to create a lift with the specified number.

Lift menu

The lift menu for the selected lift is displayed, with the first option being whether the lift is enabled.

```
1:YES - Enable
*-Change
```

Press [ENTER] to move on into the lift configuration menu.

```
1: Lift menu
0−Exit, Menu:
```

The lift menu has the following options:

- 1−Lift settings
- 2−Delete lift

1−Lift settings

Name

```
1:
(1)−Edit
```

Program a name to identify the lift. The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Press [ENTER] to move to the next option.

Remote reader

```
1:Remote reader 0
Reader No:
```

Enter the number of the remote reader and then press [ENTER]. If you want to disable the remote reader option, enter a value of [0] and then press [ENTER].

Press [ENTER] to move to the next option.

Lift access time

```
1:Lift access time 5
Access time:
```

Enter a value (1 to 255 seconds) for the lift access time from the local reader. This will determine how long the relay(s) are accessed for when a valid user accesses the Lift reader. The default value is 5 seconds.

Enter the number of seconds required, and then press [ENTER].

Press [ENTER] to move to the next option.

Remote reader access time

```
1:Remote reader access time 10
Access time:
```

Enter a value (1 to 255 seconds) for the lift access time from the remote reader. This will determine how long the relay(s) are accessed for when a valid user accesses the remote reader (if used) for this lift. The default value is 10 seconds.

Enter the number of seconds required, and then press [ENTER].

Press [ENTER] to move to the next option.

Override floor group

```
1:Override floor group 0
F/G No:
```

Enter the number of a designated floor group (1 to 128) that determines the floors that may be freely accessed in the lift controls, and the times during which they can be in access, without using a valid card or PIN at the lift reader. Enter 0 to disable an override floor group.

Enter the floor group number, and then press [ENTER].

Press [ENTER] to move to the next option.

Security floor group

```
1:Security floor group 0
F/G No:
```

Enter the number of a floor group (1 to 128) that determines the floors that may be freely accessed in the lift controls, and the times during which they can be in access, without using a valid card or PIN at the lift reader, provided that the security trigger event flag is activated (see “Security trigger event flag” below). Enter 0 to disable a security floor group.

Enter the floor group number, and then press [ENTER].

Press [ENTER] to move to the next option.

Security trigger event flag

```
1:Security trigger E/F 0
E/F No:
```

Enter a number in the range 1 to 255 for the security trigger event flag, or 0 for no security trigger. If the security trigger event flag is activated then the security floor group (see “Security floor group” above) is activated.

Enter the event flag number, and then press [ENTER].

Press [ENTER] to move to the next option.

Floor relays

A relay can be set for each of the ten floors for the lift.

```
1:Floor 1 relay: 0
Relay No:
```

Enter a relay number (from 1 to 512) for the floor, and then press [ENTER].

Press [ENTER] to move to the next floor. Once you have passed floor 10, lift settings are now fully configured.

2−Delete lift

```
Delete lift 1
0−Exit 1−Delete
```

Press [1] to delete the lift.

Option 45: Standard doors

Challenger*Plus* panels can support 32 doors, without requiring a Four-Door Controller or Network Access Controller.

A worksheet is provided to record programming details and to further describe this option. See “Standard doors worksheet” on page 286.

Door number

```
Enter door number to add/edit
Door No:
```

Enter a number in the range 1 to 126, and then press [ENTER].

Press [ENTER] to move to the next option.

Create door

If the door does not exist, the RAS will prompt you to create it.

```
1:Create door
0−Exit 1−Create
```

A maximum of 32 doors can be created. Press [1] to create a door with the specified number.

Door menu

The door menu for the selected door is displayed, with the first option being whether the door is enabled.

```
1:YES - Enable
*-Change
```

Press [ENTER] to move on into the door configuration menu.

The door menu for the selected door is displayed:

```
1: Door menu
0−Exit, Menu:
```

The door menu has the following options:

- 1−Door access options
- 2−Shunting/Passback/Egress
- 3−Alarm control
- 4−Hardware
- 5−Delete door

1−Door access options

Name

```
1:
(1)−Edit
```

Program a name to identify the door. The name may contain up to 30 characters (including spaces). To program a name via RAS, see “Programming text via RAS” on page 62.

Press [ENTER] to move to the next option.

Access time

```
1:Access time 5 sec
Time:
```

Program the amount of time for the door to unlock when a user enters a valid card or PIN at the door reader. The user is then able to open the unlocked door during the access time.

Enter the number of seconds required, and then press [ENTER].

Press [ENTER] to move to the next option.

Pre lock time

```
1:Pre lock time 2 sec
Time:
```

Once the door input has been sealed, the Challenger panel waits for the pre lock time to expire before locking the door. If the door open input unseals during the pre lock time, the door is deemed open and the pre lock timer is cancelled. The shunt continues during the pre lock time.

Enter the number of seconds required, and then press [ENTER].

Press [ENTER] to move to the next option.

Post lock time

```
Post lock time 2 sec
Time:
```

The post-lock time allows time for a lock to fully engage. After the post lock time has expired, the door is deemed secure, and the shunt is cancelled. If the door input unseals during the post lock time, the door is deemed open and the post lock timer is cancelled. The shunt continues during the post lock time.

Enter the number of seconds required, and then press [ENTER].

Press [ENTER] to move to the next option.

Override time zone

```
1:Override timezone: Not programmed
*−Dis,Tz:
```

The override time zone controls the times when the door can be opened without the need to use a valid card or PIN. Free access is allowed when the time zone is valid.

Press [*] to disable the override time zone or enter a time zone number.

Press [ENTER] to move to the next option.

Override after entry

```
1: NO − Override after entry
*−Change 0−Skip
```

This option determines whether the override time zone (see "Override time zone" section above) takes effect immediately when the time zone commences or after a user enters.

When set to YES, the override time zone takes cannot unlock the door for the programmed times unless a user has entered.

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

Report door DOTL

```
1: YES – Report door DOTL
*−Change 0−Skip
```

The door can send a report to the printer/computer when a DOTL (Door Open Too Long) condition is detected.

Press [*] to toggle the YES and NO values (enabled and disabled).

Report door FORCED

```
1: YES – Report door FORCED
*−Change 0−Skip
```

The door can send a report to the printer/computer when the door is forced (i.e. input unsealed while the door is locked).

Press [*] to toggle the YES and NO values (enabled and disabled).

Report door open/close

```
1: NO – Report door open/close
*−Change 0−Skip
```

The door can send a report to the printer/computer when the input assigned to the door is unsealed and resealed.

Press [*] to toggle the YES and NO values (enabled and disabled).

Report door secured/unsecured

```
1: NO – Report door secured/unsecured
*−Change 0−Skip
```

The door can report secured and accessed (unsecured) events. This option only functions when the hardware type is set to Maglock. It is intended to specifically report when a door is secured (closed, locked, and not shunted), as opposed to simply locked/unlocked, or opened/closed.

When this option is set to YES, whenever a user badges their card and/or access is granted on a door, the door lock will unlock and send an "unsecured" message to the management software. When the door is locked, the door input is sealed, and shunting has expired (if configured), a "secured" message will be sent to the management software.

Press [*] to toggle the YES and NO values (enabled and disabled).

2−Shunting/Passback/Egress

Shunt type

```
1: 0,No Shunting
Type:
```

This field defines shunt conditions. The options are:

Option		Function
0	No shunting	The door is not shunted.
1	Input shunting	The door is shunted. Generates an alarm, based on the input type settings, if left open longer than the programmed shunt time.
2	Input shunting & DOTL	The door is shunted as with option 1, and additionally generates a DOTL (Door Open Too Long) alarm if it is left open longer than the programmed shunt time.

Press [ENTER] to move to the next option.

Shunt time

```
1:Shunt time 60 Sec
Time:
```

Program the amount of time that the door may be opened for without causing an alarm (shunted). This allows time for a user to pass through the door and shut it again.

Enter the number of seconds required, and then press [ENTER].

Press [ENTER] to move to the next option.

Warning time

```
1:Warning time 15 Sec
Time:
```

Program the amount of time for a relay to activate, to sound a warning device, before the shunt time expires.

Enter the number of seconds required, and then press [ENTER].

Press [ENTER] to move to the next option.

Cancel shunt when door secures

```
1: NO − Cancel Shunt when door secures
*−Change 0−Skip
```

For security reasons, it may be required to limit the shunt period as much as possible in order to detect the door being opened again during the shunt time (after the debounce time of approximately 2 seconds).

Select this option to use the programmed shunt time to shunt the door input and then to cancel the shunt when the door closes (i.e. the door input is resealed).

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

Egress time zone

```
1:Egress timezone: 0
*−Dis,Tz:
```

The egress time zone controls the times when an egress button will unlock a door to allow exit. When the time zone is valid, a user can press the egress button and the door will unlock.

Press [*] to disable the egress time zone or enter a time zone number.

Press [ENTER] to move to the next option.

Egress reporting

```
1: YES − Egress reporting
*−Change 0−Skip
```

When selected, a report is sent to management software when the egress function is used.

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

3−Alarm control

Alarm group

```
1:  Alm-Grp: 1−No access
Alm-Grp:
```

Alarm groups may be assigned to doors to restrict alarm control from that door to the areas assigned to the alarm group.

Restrictions on the level of alarm control available (for example Disarm Only), and the time period (time zone) when the alarm control functions can be performed, may also be specified in the alarm group.

Enter the area alarm group number, and then press [ENTER]. See “Option 5: Alarm groups” on page 96 for details.

Press [ENTER] to move to the next option.

Alarm control type

```
1: 0,No alarm control
Type:
```

Select the type of alarm control that can be used by the door:

Option		Function
0	No alarm control	It is not possible to arm/disarm using the reader.
1	1 badge to disarm, 3 to arm	Presentation of a valid card at the reader will disarm the areas in the alarm group on first badge. Badging three times will arm the areas.

Enter a number to select the alarm control option, and then press [ENTER].

Press [ENTER] to move to the next option.

Multi badge time

```
1:Multi badge time 5 sec
Time:
```

If the reader’s alarm control options specify three-badge alarm control for users who are authorised to arm and disarm areas, you can define the amount of time permitted between the first and third badges.

If the time expires, then the user will need to repeat the three badges in order to arm or disarm the area.

Enter the number of seconds required, and then press [ENTER].

Press [ENTER] to move to the next option.

Denied if area secured

```
1: NO – Denied if area secured
*−Change 0−Skip
```

Deny access to the door if any area in the alarm group assigned to this door is secured/armed.

Press [*] to toggle the YES and NO values (enabled and disabled).

Press [ENTER] to move to the next option.

4−Hardware

Lock type

```
1: 0,Strike
Type:
```

Enter a number to select the following lock type options:

- Press [0] [ENTER] for strike.
- Press [1] [ENTER] for Maglock/Dropbolt.

Press [ENTER] to move to the next option.

Door input

```
1:Door input #1/Forced:0
Input No:
```

Enter the number of the input to be used for a door contact for the door being programmed, and then press [ENTER].

Press [ENTER] to move to the next option.

Egress input

```
1:Egress input:0
Input No:
```

This option specifies the input number that activates the egress function for the door being programmed.

Enter an input number, and then press [ENTER].

Press [ENTER] to move to the next option.

DOTL input

```
1:DOTL inpt:0
Input No:
```

This option specifies the input number that reports the DOTL (door open to long) alarm condition for the door being programmed (if DOTL is enabled in the shunting options for the door).

DOTL inputs must not have any alarm devices connected to them, and must be sealed with EOL resistors.

Enter an input number, and then press [ENTER].

Press [ENTER] to move to the next option.

Lock relay

```
1:Lock relay:0
Relay No:
```

Enter a relay number in the range 1 to 512 to activate the lock relay, and then press [ENTER].

Press [ENTER] to move to the next option.

Warning relay

```
1:Warning relay:0
Relay No:
```

Specify the relay to be activated during during the “Warning time” when the shunt timer is about to expire, e.g. may be used to activate a buzzer above a door to indicate the door needs to be closed.

Enter a relay number in the range 1 to 512, and then press [ENTER].

Press [ENTER] to move to the next option.

5−Delete door

```
Delete door 1
0−Exit 1−Delete
```

Press [1] to delete the door.

Chapter 6
Maintenance

Summary

This section provides information to help you diagnose and solve various problems that may arise while configuring or using your Interlogix product and offers technical support contacts in case you need assistance.

Content

Troubleshooting

Refer to the following tables:

- Table 19: Challenger panel help on page 214
- Table 20: RAS and Card Reader help on page 215
- Table 21: TS0820, TS0824, and TS1020 DGP help on page 216
- Table 22: TS0840 to TS0842 Relay Card help on page 217

Table 19: Challenger panel help

Condition	Possible causes
Master LCD Arming Station has all LEDs flashing and displays “Service” message.	The RAS programming option “LCD arming station” might be set to NO. The panel’s LANs may be connected incorrectly. The address on the RAS may be incorrectly set.
Panel is not communicating with RASs and/or DGPs.	The panel’s LANs may be connected incorrectly, or the wrong cable type may have been used. RAS and/or DGP numbers to be polled may not be programmed correctly or the device’s LAN address may be incorrectly set.
RASs and/or DGPs appear to be going offline and online. (Indicated by RAS/DGP fail LEDs on 16-area RAS, by LCD “RAS Fail” message, or by excessive poll errors reported).	The panel’s LANs may be connected incorrectly, or the wrong cable type may have been used. LAN termination may be incorrect. Short circuit on LAN.
Input going into alarm while area disarmed.	The programmed input type may be a 24-hr alarm or access alarm type. Input wired incorrectly causing tamper condition (open circuit or short circuit) instead of unsealed condition. EOL resistors may be installed incorrectly.
Unable to assign alarm groups when programming users.	No alarm groups have been programmed with the option “Can This Alarm Group be Assigned to Users” enabled. If a code other than the Master code (User 50) is being used to access “Program Users”, the Alarm Group assigned to it may not allow the function (you can’t assign an alarm group that has areas or menus that you don’t have).
Panel not reporting to Monitoring Station.	Communications path may be configured incorrectly. In dialler panels, the path’s account code may be programmed incorrectly. In dialler panels, the path’s phone no. 1 must be programmed.
Inputs indicating unsealed when they are sealed.	The 2K2/6K8 end-of-line resistor option is not compatible with alarm devices using normally open (NO) alarm contacts, and will result in the input indicating unsealed when it is sealed.

Table 20: RAS and Card Reader help

Condition	Possible causes
All the LEDs on the RAS are flashing.	The address recorded on the RAS may be incorrect and polling to the RAS is not being acknowledged. The LAN may be connected incorrectly. The RAS is not being polled.
LEDs are not operating.	No power or low power.
LEDs do not appear to be indicating the correct condition.	Area LEDs may be incorrectly mapped. The RAS programming option “LCD arming station” might be set incorrectly for the particular RAS. The “Disable LEDs that don't report” option may be set incorrectly.
An error is indicated (7 beeps) when a code is entered on the keypad.	An invalid PIN may have been used. The RAS may not have been programmed with an alarm group. The alarm group of the PIN may not permit access at this RAS.
A code or card is valid, but the door doesn’t unlock.	If the RAS is used to unlock a door, assign a door event flag to the RAS.
A code or card is valid, but the area doesn’t arm or disarm as expected.	The RAS’s options for “Cards auto disarm” or “Cards always disarm/arms” are set incorrectly.
A RAS has been replaced with a different model and it won’t go online.	If you disconnect an encrypted RAS and replace with a non-encrypted RAS, the RAS will not work until you depoll and repoll it.
The RAS appears to lock up when the relay which it controls via the OUT terminal, activates.	The relay probably does not have a reverse diode across it to protect against back EMF.
When you touch a TS0004 or TS0210 RAS it seems to lock up due to static.	The RAS may not have been earthed. The star washers on the cover screws may not be in place. These are used to provide an electrical connection between the cover and the base.
TS1001 RAS displays unexpected results.	Base assembly not earthed as described in *TS1001 Touch Screen Arming Station Installation Manual*, REV 03 (or later).

Table 21: TS0820, TS0824, and TS1020 DGP help

Condition	Possible causes
The “Tx” LED on the DGP is not flashing.	The links may be incorrectly set. (The address recorded on the DGP may be incorrect and polling to the DGP is not being acknowledged). The LAN cable may be connected incorrectly. The DGP is not being polled. (It may not have been included in Data Gathering Panels to be polled when programming DGPs).
“Tx” and “Rx” LEDs are not operating.	No power or low power. The LAN cable may be connected incorrectly.
The DGP appears to be going offline and online. (Indicated by “DGP Fail” on an LCD RAS or by the “DGP” LED on a TS0804 RAS).	LAN termination may be incorrect.
Some or all DGP inputs are permanently in tamper. (Or permanently in alarm if “Input Tamper Monitoring” in Install menu option 7 is set to NO).	The input numbers for the DGP have been calculated incorrectly, and input type numbers have therefore been assigned to the wrong inputs in the Input Database. The 8-Input Expansion module (if fitted) has the DIP switches incorrectly set. Additional items for TS1020 DGP: The EOL resistor setting may be incorrect. The expander type setting may be incorrect (you need to specify whether TS0021 or TS1021 modules are used). The 2K0, 1K5, and 1K0 options are not compatible with inputs connected via TS0021 Eight-Input Expansion Modules. The 2K2/6K8 option is not compatible with alarm devices using normally open (NO) alarm contacts.
Two or three Eight-Input expansion modules are fitted to increase the DGP to 24 or 32 inputs, but the 17th to 32nd inputs on the DGP do not seem to function.	DIP switch 5 on the DGP has not been set to ON. The expansion modules’ DIP switches may be set incorrectly.
4-Way Relay modules (TS0840) being used with the DGP do not function, but some of the LEDs on the module appear to be permanently on.	DIP switch 6 on the DGP is set to ON. (DIP switch 6 should only be on if 8-Way Relay modules or 16-Way Open Collector modules are being used).
8-Way Relay modules or 16-Way Open Collector modules connected to the DGP do not function.	DIP switch 6 on the DGP is set to OFF.
The siren output (with 8 ohm siren speaker connected) does not operate when it is meant to.	The 16th (last) relay number associated with the DGP address has not been mapped to a siren event flag number. The TS1020 DGP’s siren mode setting may be incorrect.

Table 22: TS0840 to TS0842 Relay Card help

Condition	Possible causes
8-Way Relay card (TS0841) won't function when connected to the Challenger panel.	The Number of Relay Controllers has not been set in Install menu option 7 - System options.
8-Way Relay card (TS0841) won't function when connected to a DGP.	DIP switch 6 has been set to OFF.
16-Way Open Collector card (TS0842) won't function when connected to the Challenger panel.	The Number of Relay Controllers has not been set in Install menu option 7 - System options.
16-Way Open Collector card (TS0842) won't function when connected to a DGP.	DIP switch 6 has been set to OFF.
4-Way Relay card (TS0840) won't function when connected to the Challenger panel.	The number of relay controllers has not been set to 0 in Install menu option 7 - System options.
4-Way Relay card (TS0840) won't function when connected to a DGP.	The card’s DIP switch 6 has been set to ON.
Relays will not function after being enabled as above.	The relay has not been mapped to an Event Flag or the relay number has been calculated incorrectly and therefore not programmed as the correct relay number. The relay is being held inactive during a time zone. The cable has been connected incorrectly, or is the wrong cable for the application. There are too many relay boards being powered from the Challenger panel’s J14 connector (the panel can power one relay board only). The relay board’s LED will appear dim or off if relays are drawing too much power. You will need to turn all relays off before you can recover from fuse fail condition.

Maintenance

Introduction

This section outlines the Interlogix recommended maintenance for Challenger panels.

Standards

Routine maintenance on intruder alarm systems installed in a client’s premises should be performed in accordance with AS/NZS 2201.1-2007 SECTION 5 MAINTENANCE AND SERVICE, and SECTION 6 RECORDS AND REPORT.

Copies of this standard are available from Standards Australia and can be purchased online (Standards Australia web site: http://www.standards.org.au/).

Peripheral devices

Specific routine maintenance procedures for individual items of peripheral devices connected to the Interlogix equipment are not included in this procedure. “Peripheral devices” include, but are not limited to, movement detectors, smoke detectors, warning devices, batteries, and access readers.

Note that operation of most peripheral devices will be performed as part of the test procedures required in this maintenance procedure. However, this may or may not meet the routine maintenance procedures recommended by the suppliers or manufacturers of those devices.

If required, obtain routine maintenance procedures for peripheral devices from the suppliers or manufacturers of those devices. As a minimum, follow the procedure described in AS/NZS 2201.1-2007 relating to:

- Detection devices
- Audible and visible alarm and warning devices

Automated testing

Refer to the following sections for details of system features that can be used to provide some automated system testing:

- Input Test Type — See “Option 1: Input database” on page 70.
- Siren Output Test — See “Option 7: System options” on page 108.
- Periodic Dialler Test Reports — See “Option 9: Communications” on page 122.
- Dynamic Battery Testing — See “Option 31: Battery testing” on page 179.

These automated functions are not designed to replace any of the routine maintenance procedures, but will further enhance the integrity of the system during normal day-to-day operation.

Recommended routine maintenance procedures

Table 23: Challenger system routine maintenance schedule

Task	Frequency	Description
Notify the monitoring company	As required	If the system is monitored, the central monitoring station (CMS) staff must be notified before any tests are made. To perform testing and/or maintenance work on monitored systems, you must be authorised to do so. Central stations have procedures for identifying authorised personnel.
Notify personnel on the premises	As required	Prior to any test that will impact on any personnel, ensure that all affected personnel and appropriate supervisory and/or management staff are given any necessary notification, warning or instructions (for example, testing of zone inputs and warning devices).
Check the equipment schedule	Once per year	Check the installation, location and siting of all equipment and devices against the records supplied by the installation company. Record and report any discrepancy.
Check the wiring and conduits	Once per year	Inspect all visible wiring and conduits.
Check for dust, moisture and vermin	Once per year	Check for ingress of dust, moisture, condensation and vermin into all equipment enclosures. If excessive moisture or foreign matter is present, check enclosure location, environment, mounting method and cable entry points for sources of entry, and take steps to rectify.
Check the power supply	Once per year	Check that all mains operated modules and power supplies are connected to a mains outlet and are operational.
Check the Challenger 2 A power supply output voltage 13.8 V ± 2%	Once per year	Test DC voltage across the “+” and “-” output terminals on all power supplies, with battery disconnected.
Check the detector supply voltage 13.8 V ± 2%	Once per year	Test DC voltage across the “Auxiliary Power Output” terminals on the following equipment: • Challenger panel • Standard input data gathering panels • Intelligent 4-Door/4-Lift Controllers
Check batteries	Once per year	Check that all battery-backed panels and power supplies have the battery fitted and connected to the “Batt +” and “Batt -” terminals. • Challenger panel • Standard input DGPs • Intelligent 4-Door/4-Lift Controllers • Power supplies (battery backed)

Task	Frequency	Description
Test battery charge voltage 13.8 V ± 2%	Once per year	Test DC voltage on the “Batt +” and “Batt -” terminals. • Challenger panel • Standard input DGPs • Intelligent 4-Door/4-Lift Controllers • Power supplies (battery backed) **NOTE**: When mains power is restored following an AC fail condition, the battery charge voltage may range from 11 V to 13.8 V while the battery is recharging.
Replace battery	As specified by the battery manufacturer — OR — no more than 3 years	Replace the sealed lead-acid battery with a battery of the same specifications. Record the installation date of the new battery where it is clearly visible on the battery itself, or on a label clearly visible within the equipment enclosure and in the system maintenance records.
Check LCD/LED RAS keypad keys	Once per year	Check operation of every key on the keypad. Observe that labelling on all keys is clearly legible. Observe that keypad backlighting is operational on supported keypads.
Check LCD/LED RAS keypad displays	Once per year	Observe all LCD characters are operational. Observe LCD backlight is operational. Test operation of each LED on RAS terminals. See “Option 12: Lamp test” on page 160.
Check LCD/LED RAS egress and output	Once per year	If the RAS egress or output is used then test their operation. The egress should open the door and the output should activate when required.
Test operation of access reader inputs and outputs	Once per year	Test the operation of all access readers using appropriate user ID tokens, including card, key fob, PIN, and so on. Results of reader operation and response of reader LEDs and beeper will depend on system programming. The required operation and test method should be recorded in the system maintenance records.
Test the secondary (backup) communications format (if provided)	As agreed between the alarm company and the client, but not less that once per year. Also see “Notes” on page 222.	**NOTE**: Must be pre-arranged in consultation with the CMS staff. • Disconnect the primary (main) communications format. • Perform an operation that triggers reporting. • Check that, after attempting to communicate via the primary format, the system reports successfully via the secondary format. • Re-connect the primary communications format.

Task	Frequency	Description
Test the primary (main) communications format. (May be performed in conjunction with zone input testing).	As agreed between the alarm company and the client, but not less than once per year. Also see “Notes” on page 222.	**NOTE**: Must be pre-arranged in consultation with the CMS staff. • Perform an operation that triggers reporting. • Check that the system reports successfully.
Test system inputs (detection devices). Test areas programmed to Report. **NOTE**: Special testing devices or procedures may be required if testing of smoke, heat, seismic glass-break detectors, and so on, is required.	As agreed between the alarm company and the client, but not less than once per year. Also see “Notes” on page 222.	• Obtain a list of all inputs to be tested. • Test each input by causing it to switch from the sealed state to un-sealed (alarm) and back to sealed. • The Test Input user menu can be used to monitor the zone activity. • Check-off each input on the list as it is successfully tested. • Record and report any discrepancy. Many alarm companies recommend that input testing includes reporting the zone input alarms to the central station to fully test the alarm system operation. When this type of testing is required, the following points must be noted: • The testing must be pre-arranged in consultation with the CMS staff. • All the relevant areas must be turned on. • After testing, turn the relevant Areas off again. • Obtain the central station report of all input alarms/restores and area opens/closes reported during the testing procedure. • Compare the input/area list and central station report to ensure that all tested inputs reported alarm and restore, and all tested areas reported close and open as required. • Record and report any discrepancy.
Test warning device outputs. (May be performed in conjunction with zone input testing).	As agreed between the alarm company and the client, but not less than once per year. Also see “Notes” on page 222.	**NOTE**: The CMS staff may need to be notified before these tests are made. Test the operation of each audible and visible warning device. • Turn on the appropriate area. • Activate a detection device or user operation that is programmed to trigger the warning device. • Check that the warning device operates as specified. • Record and report any discrepancy.
Backup history files for management software (for example, CTPlus or Forcefield).	Recommended monthly	Backups should be performed on a regular basis depending on the number of events. The backup file should be verified and then the same data should be purged or deleted from the database.

Task	Frequency	Description
Backup or export database for management software (for example, CTPlus or Forcefield).	Recommended monthly	Database backups or exports should be performed on a regular basis. Verify that the backup file has been created.
Perform modifications	As required	Any modifications to the system as a result of the maintenance procedure must be recorded and reported. Technician to program next service date. See "Option 33: Program next service" on page 182.
Obtain client approval	At the conclusion of every routine maintenance visit	Obtain the signature of the client or the client's representative on the maintenance record.

Notes

The frequency for testing the operation of all detection devices, audible and visible alarm warning devices and remote signalling (reporting) operations should be determined according to the needs of the particular installation.

AS/NZS 2201.1-2007 specifies that these tests must be carried out at least once per year (depending on site), however some central stations and clients prefer more frequent testing to ensure the integrity of the system. For example:

- Sites requiring a higher level of security monitoring, or that are prone to interference of harsh environmental conditions, may choose to have these tests carried out quarterly or more frequently.
- Very large sites with hundreds of detection devices may choose to do testing every 6 months with 50% of the detection devices tested on each visit.

Sites where the automated testing functions in the product have been enabled and properly implemented may find that annual routine maintenance is adequate.

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, please contact your Installation Company or distributor, as applicable.

Note: Be ready at the equipment before calling for technical support.

Appendix A
Reference materials

Content

System numbering

Overview

All DGPs, zone inputs, relays (outputs), doors, and lifts are numbered according to a set formula. This is used when determining the physical numbers and locations when programming.

Zone input numbering

A Challenger system can receive alarm signals from up to 1008 zone inputs. The Challenger panel itself has 16 zone input connections. Additional zone inputs may be provided by Data Gathering Panels (DGPs), Wireless Data Gathering Panels (WDGPs) and Intelligent Access Controllers on the system LAN. This section will refer to all of these devices as DGPs, unless otherwise noted.

Every DGP is assigned a DGP address in the range 1 to 15 (on LAN 1) and 17 to 32 (on LAN 2). Intelligent Access Controllers may use the first 12 addresses on each LAN.

The Challenger numbering scheme allocates 32 zone inputs per DGP address for a theoretical total of 1008 zone inputs (including the panel’s 16 zone inputs).

Note: TS0866, TS0867, and TS0869 Intelligent Access Controllers can use 16 zone input connections; the TS0827 Four-Input DGP can use 4 zone input connections. The system total of 1008 zone inputs is reduced accordingly when these products are used.

Table 24 below lists the standard and expanded input capacities for various DGPs.

Table 24: Input connection options for DGP devices

DGP Model	Type	Onboard inputs	Expanded inputs
TS1020	8-input analogue DGP	8	32 (using 3 of TS1021)
TS0820, TS0824	8-input standard DGP	8	32 (using 3 of TS0021)
TS0827	4-input DGP	4	not applicable
TS0825, TS0825E, CA1230	Wireless DGP	16 wireless inputs	32 wireless inputs
TS0866	Intelligent 4-Door Controller	8	16 (using 1 of TS0021)
TS0867	Intelligent 4-Door Controller	16	not applicable
TS0869	Intelligent 4-Lift Controller	16	not applicable

The Challenger panel has inputs and relays numbered 1 to 16. DGP input and relay numbers are assigned according to Table 25 below.

Table 25: DGP addressing, DPG DIP switches, and input and relay numbering

LAN	Address	Polled as	SW1	SW2	SW3	SW4	Inputs	Relays
LAN 1	DGP 1	DGP 1	I	O	O	O	17 to 48	17 to 32
LAN 1	DGP 2	DGP 2	O	I	O	O	49 to 80	33 to 48
LAN 1	DGP 3	DGP 3	I	I	O	O	81 to 112	49 to 64
LAN 1	DGP 4	DGP 4	O	O	I	O	113 to 144	65 to 80
LAN 1	DGP 5	DGP 5	I	O	I	O	145 to 176	81 to 96
LAN 1	DGP 6	DGP 6	O	I	I	O	177 to 208	97 to 112
LAN 1	DGP 7	DGP 7	I	I	I	O	209 to 240	113 to 128
LAN 1	DGP 8	DGP 8	O	O	O	I	241 to 272	129 to 144
LAN 1	DGP 9	DGP 9	I	O	O	I	273 to 304	145 to 160
LAN 1	DGP 10	DGP 10	O	I	O	I	305 to 336	161 to 176
LAN 1	DGP 11	DGP 11	I	I	O	I	337 to 368	177 to 192
LAN 1	DGP 12	DGP 12	O	O	I	I	369 to 400	193 to 208
LAN 1	DGP 13	DGP 13	I	O	I	I	401 to 432	209 to 224
LAN 1	DGP 14	DGP 14	O	I	I	I	433 to 464	225 to 240
LAN 1	DGP 15	DGP 15	I	I	I	I	465 to 496	241 to 256
LAN 2	DGP 1	DGP 17	I	O	O	O	497 to 528	257 to 272
LAN 2	DGP 2	DGP 18	O	I	O	O	529 to 560	273 to 288
LAN 2	DGP 3	DGP 19	I	I	O	O	561 to 592	289 to 304
LAN 2	DGP 4	DGP 20	O	O	I	O	593 to 624	305 to 320
LAN 2	DGP 5	DGP 21	I	O	I	O	625 to 656	321 to 336
LAN 2	DGP 6	DGP 22	O	I	I	O	657 to 688	337 to 352
LAN 2	DGP 7	DGP 23	I	I	I	O	689 to 720	353 to 368
LAN 2	DGP 8	DGP 24	O	O	O	I	721 to 752	369 to 384
LAN 2	DGP 9	DGP 25	I	O	O	I	753 to 784	385 to 400
LAN 2	DGP 10	DGP 26	O	I	O	I	785 to 816	401 to 416
LAN 2	DGP 11	DGP 27	I	I	O	I	817 to 848	417 to 432
LAN 2	DGP 12	DGP 28	O	O	I	I	849 to 880	433 to 448
LAN 2	DGP 13	DGP 29	I	O	I	I	881 to 912	449 to 464
LAN 2	DGP 14	DGP 30	O	I	I	I	913 to 944	465 to 480
LAN 2	DGP 15	DGP 31	I	I	I	I	945 to 976	481 to 496
LAN 2	DGP 16	DGP 32	O	O	O	O	977 to 1008	497 to 512

Legend: I = ON, O = OFF

Notes:

- Input numbers in the range 1000 to 1008 will not report CID alarms.
- The Challenger panel is assigned input numbers 1 to 16.
- The Challenger panel is assigned relay numbers 1 to 16 (more with potential duplication). Relay 2 is assigned to the panel’s strobe.
- The siren output is the highest relay number assigned to the DGP address.
- Challenger V8 DGP installation instructions may say “Set the first four segments to OFF to disable the DGP”. This does not apply to DGPs used on LAN 2, where you set the first four segments to OFF for DGP 16.

Relay and output numbering

Relay numbers are used for physical relays, for logical outputs such as used in macros, and for open collector outputs and LEDs.

Challenger panels support 512 relays:

- Panel relays numbered 1 to 16 (relay 2 operates the strobe). Higher relay numbers can be used at the risk of duplication (for example, relay 17 on both the panel and DGP 1 can activate simultaneously).
- LAN 1 can have 15 DGPs with relays numbered 17 to 256.
- LAN 2 can have 16 DGPs with relays numbered 257 to 512.
- Each DGP address uses the 16th relay number for the siren output.

In Challenger, the number that a relay uses depends on where it is used:

- When programming the relay in the Challenger panel, the DGP address must be considered (for example, the first relay on DGP 1 is relay 17).
- When programming an Intelligent Access Controller's physical relays, the DGP address is already known, so the relays for any address are numbered from 1.

Note: If you want to control an Intelligent Access Controller's physical relay from the Challenger panel, you need to use the relay’s macro event number as an input for a DGP macro logic program (refer to the Intelligent Access Controller's programming manual for details).

Relay numbers are assigned according to Table 25 on page 225.

If the Challenger panel has more than 16 relays, then the numbering system allows for duplication between the Challenger panel’s relays and a DGP’s relays.

Example:

- The Challenger panel has three TS0841 8-way relay controllers, so it has 23 relays numbered 1 to 24 (relay 2 is assigned to the panel’s strobe).

- DGP 1 (TS0820) has one TS0841 8-way relay controller, so it has 16 relays numbered 17 to 32.
- The relay numbers 17 to 24 apply to both the panel and the DGP. The result of this duplication is that any relays that share a number will both be active (or inactive) simultaneously.

Siren output numbering

The siren output is the highest relay number assigned to the DGP address.

The internal and external siren speaker outputs on Challenger panels are always treated as relay 16. On DGPs with siren speaker outputs, the last of the 16 relay numbers associated with that DGP address is the siren output. For example, on LAN 1, DGP 3, the siren speaker output is relay 64.

To enable the siren speaker output, the relay number representing the siren output must be mapped to the required siren event flag number. The default mapping is event flag 1. Siren event flag numbers are programmed in “Option 2: Area database” on page 77.

Door and lift numbering

Door and lift numbers are determined by:

- The RAS or reader address when connected to the Challenger system LANs (doors 1 to 16 and 65 to 80). These doors are reserved for RASs 1 to 16 and 65 to 80, and provide only basic access control (door opening).
- The Intelligent Access Controller address when connected to the local LAN (doors 17 to 64 and 81 to 128). These door and lift numbers are controlled by Intelligent Access Controllers, and provide enhanced access control functions such as anti-passback.

Refer to Table 26 below for details of door and lift numbering.

Table 26: Door and lift numbers allocated per DGP

Device and address	First door or lift	Second door or lift	Third door or lift	Fourth door or lift
LAN 1, RAS 1 to 16			Doors 1 to 16	
LAN 1, DGP 1	17	18	19	20
LAN 1, DGP 2	21	22	23	24
LAN 1, DGP 3	25	26	27	28
LAN 1, DGP 4	29	30	31	32
LAN 1, DGP 5	33	34	35	36
LAN 1, DGP 6	37	38	39	40
LAN 1, DGP 7	41	42	43	44

Device and address	First door or lift	Second door or lift	Third door or lift	Fourth door or lift
LAN 1, DGP 8	45	46	47	48
LAN 1, DGP 9	49	50	51	52
LAN 1, DGP 10	53	54	55	56
LAN 1, DGP 11	57	58	59	60
LAN 1, DGP 12	61	62	63	64
LAN 2, RAS 65 to 80	Doors 65 to 80			
LAN 2, DGP 17	81	82	83	84
LAN 2, DGP 18	85	86	87	88
LAN 2, DGP 19	89	90	91	92
LAN 2, DGP 20	93	94	95	96
LAN 2, DGP 21	97	98	99	100
LAN 2, DGP 22	101	102	103	104
LAN 2, DGP 23	105	106	107	108
LAN 2, DGP 24	109	110	111	112
LAN 2, DGP 25	113	114	115	116
LAN 2, DGP 26	117	118	119	120
LAN 2, DGP 27	121	122	123	124
LAN 2, DGP 28	125	126	127	128

Although standard DGPs are numbered 1 to 16, Intelligent Access Controllers are numbered from 1 to 12, therefore a Challenger system can only have 12 Intelligent Access Controllers on each LAN (24 in total).

Time zone numbering

A time zone (‘hard’ time zone) is a program setting that identifies specific time periods on specific days. Time zones are allocated to security system functions to control the activity of that function by time and day and are primarily used to restrict access.

Time zones are numbered 1 to 24 and 42 to 63, and are programmed for specific time periods. Each time zone is made up of one to eight sub-time zones.

Soft time zones are numbered 26 to 41 and are active only when a relay is active (they are based on events instead of on time).

Table 27 on page 229 lists the hard and soft time zones that can be used in a Challenger system.

Table 27: Time zone application

Number	Type	Application
0	24-hour	Always valid, cannot be edited.
1 to 24, 42 to 63	Hard	Use wherever you need to define up to eight sub-time zones containing a start time, an end time, the weekdays that the sub-time zone is valid, and an option to make the sub-time zone valid on specified holiday types. See “Option 13: Time zones” on page 161.
25	Service	Use to enable the service technician’s PIN or card, and can also be used to enable or disable any other system functions such as relays that are required while the service technician is in attendance. See “Programming service technician access” on page 53.
26 to 41	Soft	Soft time zones are active only when a relay or output is active. See Option 22: Soft time zones on page 175.

Input types

Input types may be grouped by their basic functionality as follows:

- Access alarms—Inputs that will only generate an alarm when one or more of the areas assigned are in access (disarmed). Refer to input types 1 and 11.
- Secure alarms – Inputs that will only generate an alarm when all of the areas assigned are in secure (armed). Refer to input types 2, 3, 4, 13, 14, 28, 60, 61, and 62.
- 24-hour alarms—Inputs that will generate the same alarm regardless of area status. Refer to input types 5, 29, 33, and 59.
- Access/secure alarms—Inputs that will generate different types of alarms when in access and secure. Refer to input types 8, 15, 21, 22, 30, 40, 41, 42, 44, 45, 46, 47, and 56.
- Area control—Inputs that turn areas on and off. Refer to input type numbers 6, 31, 34, and 35. These inputs do not have areas assigned to them. Their functions are determined by assigning an alarm group to them.
- Activate event flag only—Inputs that activate event flags but do not generate alarms. Refer to input types 7, 20, 32, and 43.
- Activate report only—Inputs that activate reports but do not generate alarms. Refer to input types 27 and 57.
- Special purpose—Special input types for system functions. Refer to input types 9, 12, 16, 18, 19, and 58.
- Camera monitoring—Panel inputs 1 to 16 only (not DGP inputs) that monitor camera film levels. Refer to input types 23, 24, 25, 26, 36, 37, 38, 39, 48, 49, 50, 51, 52, 53, 54, and 55.

Input tamper monitoring

The system option “Input tamper monitoring” determines whether the Challenger panel can detect two input states (sealed and unsealed) or four input states (sealed, unsealed, open, and short), as follows:

- When input tamper monitoring is enabled, open or short conditions are both reported as an input tamper alarm (subject to input type).
- When input tamper monitoring is disabled, then an open or short circuit will be treated as unsealed.

Certain input types use the open and short conditions for their functions, in which case input tamper monitoring may not be possible (or is limited). Input types 7, 12, 20, 27, 23, 24, 25, 26, 36, 37, 38, 39, 48, 49, 50, 51, 52, 53, 54, 55, 57, 58, are affected.

Application notes

- Do not use input type 17.
- Input type 10 is designated ‘spare’ and has no functionality.
- An input is in access when any of the areas assigned to it are disarmed.
- An input is in secure when all of the areas assigned to it are armed.
- Disarming a total disarm area (or area group) prevents alarm input types from generating alarms (except to indicate input tamper, if input tamper monitoring is used). See “Total disarm” on page 108.
- The exit timer suppresses alarms from entry/exit input types (3, 4, 13, 14, 41, 42, 61, and 62) but does not suppress alarms from other inputs. See “Enable exit fault reporting” on page 120 to report alarms from non-entry/exit type inputs as “exit error alarms”.
- The input type can affect the input’s programmed event flag and event selections. For example, input types that activate event flags only (7, 20, 32, and 43) do not generate alarms, so alarm-based event flags won’t work. Camera count input types do not activate event flags, but camera film out input types will activate a programmed event flag. Refer to “Programming input event flags” on page 73 for more details.
- There are three twin trip input types (60, 61, and 62). See “Programming twin trip inputs” on page 65 for more information.

List of input types

Table 28 on page 231 lists the input types grouped by basic functionality. Refer to the Index for a list of input types by number.

The column *Name* is an expanded version of what is displayed on an LCD RAS. For example, the name of input type 44 on a RAS is “(Acc.Loc/Sec.Alm) Dis

Cln.Tr”. This name is shown here as “Access local/secure alarm disabled by cleaners or trades”.

Table 28: Input types

Input type	Name	Description
0	none	No input type programmed. The physical input does not exist. **Note:** This is the default type for inputs 17 to 1008. Input type 0 is not retrieved to management software.
Access alarms—Inputs that will only generate an alarm when one or more of the areas assigned are in access (disarmed). Refer to input types 1 and 11.		
1	Access alarm	In access an unsealed input generates an alarm. *Example*: Hold-up button
11	Delayed access alarm	In access an unsealed input starts the delay holdup timer and the RAS indicates alarm condition (but the alarm is not reported). An alarm is reported if a second delayed access alarm is unsealed (in any area) or if the delayed holdup timer expires. *Example*: Hold-up button to report after a delay. *Programming*: Delay holdup time.
Secure alarms – Inputs that will only generate an alarm when all of the areas assigned are in secure (armed). Refer to input types 2, 3, 4, 13, 14, 28, 60, 61, and 62.		
2	Secure alarm	In secure an unsealed input generates an alarm. *Example*: Internal door, PIR (motion detector). **Note:** This is the default type for inputs 1 to 16.
3	Entry exit alarm	In secure an unsealed input generates an alarm when the entry and exit timers for the areas assigned to the input have expired. When the area changes to secure the exit timer starts. Unsealing the input during the exit time will not generate an alarm. If the input is unsealed after the exit time has expired, then the entry timer starts. Unsealing the input during the entry time will not generate an alarm. An alarm is generated if the input is still unsealed when the entry time expires. *Example*: Front door. *Programming*: Area entry and exit times.
4	Entry exit handover alarm	In secure an unsealed input generates an alarm when the exit timer for the input has expired and the entry timer is not running. *Example*: PIR at entrance. *Programming*: Area entry and exit times.
13	Entry exit no seal check	In secure an unsealed input generates an alarm when entry/exit timers have expired. The input does not need to be sealed when turning the area to secure. *Programming*: Area entry and exit times.
14	Entry exit handover alarm no seal check	In secure an unsealed input generates an alarm when the exit timer has expired and the entry timer is not running. The input does not need to be sealed when turning the area to secure. *Programming*: Area entry and exit times.

Input type	Name	Description
28	Non-latching secure alarm	In secure an unsealed input generates an alarm. The alarm resets automatically when the input seals. *Example*: PIR **Note:** Unlike previous Challenger versions, the input must be sealed (or isolated) before the area can be armed.
60	Twin trip secure alarm	In secure, generates an alarm if input unsealed a second time within the maximum twin trip time. *Example*: PIR (motion detector). *Programming:* Maximum twin tip time.
61	Twin trip entry exit handover	In secure, generates an alarm if input unsealed a second time within the maximum twin trip time, provided the exit timer for the input has expired and the entry timer is not running. *Example*: PIR at entrance. *Programming*: Area entry and exit times, and maximum twin trip time.
62	Twin trip handover no seal check	In secure, generates an alarm if input unsealed a second time within the maximum twin trip time, provided the exit timer has expired and the entry timer is not running. The input does not need to be sealed when setting the area to secure. *Programming*: Area entry and exit times, and maximum twin trip time.
24-hour alarms—Inputs that will generate the same alarm regardless of area status. Refer to input types 5, 29, 33, and 59.		
5	24-hour alarm	In access or secure, an unsealed input generates an alarm. *Example*: Panel tampers, panic alarm.
29	24-hour non-latching alarm	In access or secure, an unsealed input generates an alarm. The alarm resets automatically when the input seals.
33	24-hour alarm & isolate input	In access or secure, an input can report an alarm, a tamper condition, or be isolated: • Shorted – generates an alarm • Sealed – no alarm generated • Unsealed – isolate (no alarm generated) • Open – generates a tamper alarm *Example*: A key switch is used to isolate the input in shopping centres where only one input is available for each shop. **Note:** The input's "Activate Selected Event on Unseal" option does not apply to this input type.
59	24-hour alarm disabled by time zone 41	An input with this type is disabled when soft time zone 41 is activated by a relay (no local alarm, alarm or tamper can be generated). If the input is still unsealed when time zone 41 becomes invalid an alarm will not be generated unless the input seals and is unsealed again. In access or secure (when time zone 41 is not valid) an unsealed input generates an alarm. *Programming*: Link soft time zone 41 to a relay (see “Option 22: ” on page 175).

Input type	Name	Description
Access/secure alarms—Inputs that will generate different types of alarms when in access and secure. Refer to input types 8, 15, 21, 22, 30, 40, 41, 42, 44, 45, 46, 47, and 56.		
8	Delayed access/ secure alarm	In access an unsealed input starts the delay holdup timer and the RAS indicates alarm condition (but the alarm is not reported). An alarm is reported if a second delayed access alarm is unsealed (in any area) or if the delayed holdup timer expires. In secure an unsealed input generates an alarm. *Example*: Hold-up button on a counter where more than one hold-up button is used. *Programming*: Delay holdup time.
15	Access local/secure alarm	In access an unsealed input generates a local alarm ("Local Alarm" is displayed and the beeper sounds on RASs assigned to the same areas). The local alarm can be reset via RAS by pressing [ENTER] [ENTER] 0 [ENTER], or USER CODE [OFF] AREA [ENTER] to stop the audible alert and cancel the event. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. In secure an unsealed input generates an alarm. *Example*: Emergency exit. *Programming*: Local alarm reminder time.
21	Access local (code to reset)/ secure alarm	In access an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). An authorised user code is required to reset the silent local alarm via RAS by pressing USER CODE [OFF] AREA [ENTER]. If the input remains unsealed, it will re-alarm after the programmed local alarm reminder time. In secure an unsealed input generates an alarm. *Example*: Emergency door. *Programming*: Local alarm reminder time.
22	Access delayed non-latching/ secure alarm	In access an unsealed input starts the delay holdup timer and the RAS indicates alarm condition (but the alarm is not reported). If the input reseals before the delay holdup timer expires, then the alarm automatically resets. An alarm is reported if a second delayed access alarm is unsealed (in any area) or if the delayed holdup timer expires. In secure an unsealed input generates an alarm. *Example*: Hold-up button. *Programming*: Delay holdup time.
30	Access local non-latching/ secure alarm	In access an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). The alarm automatically resets when the input seals. In secure an unsealed input generates an alarm. The alarm does not automatically reset when the input seals. *Example*: Emergency door.

Input type	Name	Description
40	Access suspicion or delayed holdup/ secure alarm	In access an unsealed input starts the delay holdup timer and the RAS indicates alarm condition (but the alarm is not reported). An alarm is reported if a second delayed access alarm is unsealed (in any area) or if the delayed holdup timer expires. A shorted input activates cameras in the areas that are assigned to the input. When the input switches back to sealed, the cameras continue to operate for the suspicion time. An open input reports a tamper. In secure an unsealed input generates an alarm. *Programming*: Delay holdup time, suspicion time.
41	Access local/ entry exit alarm	In access an unsealed input generates a local alarm (“Local Alarm” is displayed and the beeper sounds on RASs assigned to the same areas). The local alarm can be reset via RAS by pressing [ENTER] [ENTER] 0 [ENTER], or USER CODE [OFF] AREA [ENTER] to stop the audible alert and cancel the event. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. In secure an unsealed input generates an alarm when the entry/exit timers for the areas assigned to the input have expired. *Example*: Emergency door that is also used to enter the premises. *Programming*: Area entry and exit times, local alarm reminder time.
42	Access local (code to reset)/entry exit alarm	In access an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). The silent local alarm can be reset via RAS by pressing USER CODE [OFF] AREA [ENTER]. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. In secure an unsealed input generates an alarm when the entry/exit timers for the areas assigned to the input have expired. *Example*: Emergency door that is also used to enter the premises. *Programming*: Local alarm reminder time, area entry and exit times.
44	Access local/secure alarm disabled by cleaners or trades	In access an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). The silent local alarm can be reset via RAS by pressing USER CODE [OFF] AREA [ENTER]. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. If a user with user category 2 or user category 6 in their alarm groups enters their code to put the area in access, then an unsealed input does not generate a silent local alarm. In secure an unsealed input generates an alarm. *Example*: Emergency door. *Programming*: Local alarm reminder time. If you want to disable the silent local alarm in access (for certain users), then program a user category (2 or 6), the user category time, and the user’s alarm group.

Input type	Name	Description
45	Access event flag/secure alarm disabled by cleaners or trades	In access an unsealed input activates the input's event flag. If a user with user category 2 or user category 6 in their alarm groups enters their code to put the area in access, then an unsealed input does not activate the input's event flag. In secure an unsealed input generates an alarm. *Example*: Emergency door. *Programming*: Input event flag number. If you want to disable the event flag in access (for certain users), then program a user category (2 or 6), the user category time, and the user's alarm group.
46	Access alarm/secure alarm	In access an unsealed input generates an alarm (this is normal functionality where the alarm is determined by the input's programmed report ID number). In secure an unsealed input reports a general alarm (CID 140) regardless of the input's programmed report ID number.
47	Suspicion holdup/ secure alarm	In access an unsealed input generates an alarm (this is normal functionality where the alarm is determined by the input's programmed report ID number). A shorted input activates cameras in the areas that are assigned to the input. When the input switches back to sealed, the cameras continue to operate for the suspicion time. An open input reports a tamper. In secure an unsealed input reports a general alarm (CID 140) regardless of the input's programmed report ID number. *Programming*: Suspicion time.
56	Access local (code to reset)/secure alarm, disabled by time zone 41	An input with this type is disabled when soft time zone 41 is activated by a relay (no local alarm, alarm or tamper can be generated). If the input is still unsealed when time zone 41 becomes invalid an alarm will not be generated unless the input seals and is unsealed again. In access (when time zone 41 is not valid) an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). The silent local alarm can be reset via RAS by pressing USER CODE [OFF] AREA [ENTER]. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. In secure (when time zone 41 is not valid) an unsealed input generates an alarm. *Example*: Emergency door. *Programming*: Local alarm reminder time, and link soft time zone 41 to a relay (see "Option 22: " on page 175).
Area control—Inputs that turn areas on and off. Refer to input type numbers 6, 31, 34, and 35. These inputs do not have areas assigned to them. Their functions are determined by assigning an alarm group to them.		
6	Area control input	An unsealed (momentary) input performs the programmed alarm group functions, such as arming an area. *Example*: Push button for quick arming on exit (the alarm group should allow arm but not disarm). *Programming*: Alarm group.

Input type	Name	Description
31	Area control on-off	An unsealed input secures the area. A sealed input puts the area in access. This input types uses an alarm group to perform the arm/disarm functions. *Example*: Latching key switch to arm and disarm areas. *Programming*: Alarm group.
34	Area disarm/user category arm	When disarmed, switching from sealed to unsealed starts the warning time. As long as the input remains unsealed, the RAS beeps and displays the user category name followed by “ending”. The area arms when the warning time expires. When armed, switching from unsealed to sealed disarms the area. *Example*: Latching key switch used to arm and disarm. *Programming*: Warning time, a user category, and the input’s alarm group.
35	Area user category arm only	When disarmed, unsealing the input starts the warning time. The RAS beeps and displays the user category name followed by “ending”. The area arms when the warning time expires. *Example*: Push button used to arm but not disarm. *Programming*: Warning time, a user category, and the input’s alarm group.
Activate event flag only—Inputs that activate event flags but do not generate alarms. Refer to input types 7, 20, 32, and 43.		
7	Camera suspicion input	An unsealed input activates the film cameras in the areas assigned to the input. When the input reseals, the cameras continue to operate for the suspicion time. *Example*: Suspicion button. *Programming*: Suspicion time. **Note:** This input type cannot indicate tamper.
20	Input to activate event flag 24-hour	In access or secure an unsealed, opened, or shorted input activates the input’s event flag. *Example*: Doorbell. *Programming*: Input event flag number. **Note:** This input type cannot indicate tamper.
32	Input to activate event flag in secure	In secure an unsealed input activates the input’s event flag. *Example*: Temperature alarm on freezer activates buzzers. *Programming*: Input event flag number. **Note:** This input type can indicate tamper on open or short when its area is disarmed (access).
43	Input to activate event flag in access	In access an unsealed, opened, or shorted input activates the input’s event flag. *Example*: Buzzer to indicate that a closet door is open. *Programming*: Input event flag number. **Note:** This input type can indicate tamper on open or short when its area is armed (secure).

Input type	Name	Description
Activate report only—Inputs that activate reports but do not generate alarms. Refer to input types 27 and 57.		
27	Input to activate report	In access or secure an unsealed, open, or shorted input reports an alarm to management software and central station, but does not indicate an alarm condition on the RAS. The alarm automatically resets when the input reseals. *Example*: Temperature alarm on freezer. **Note:** This input type cannot indicate tamper.
57	Input to report and screen	In access or secure an unsealed, open, or shorted input reports an alarm to management software and central station, but does not indicate an alarm condition on the RAS (however, it displays the system's event text via LCD RAS). The alarm automatically resets when the input reseals. *Example*: Temperature alarm on freezer. *Programming*: Event text. **Note:** This input type cannot indicate tamper.
Special purpose—Special input types for system functions. Refer to input types 9, 12, 16, 18, 19, and 58.		
9	Reset delayed input	When unsealed this input type resets a delayed alarm from input types (8, 11, 22, and 40) where the input has been resealed or the delay timer is still running (a full alarm has not been generated). If the delayed input is still unsealed, then it stops the cameras from operating but the delayed time continues to run. *Example*: Reset button for quick cancellation of alarm.
12	Courier restart	This is a pulsed key switch that resets the entry timers and restarts the exit timers for all areas assigned to the input. *Example*: Key switch next to door.
16	24-hour local mains fail	In access or secure, an unsealed input generates a local alarm ("Local Alarm" is displayed and the beeper sounds on RASs assigned to the same areas). The local alarm can be reset via RAS by pressing [ENTER] [ENTER] 0 [ENTER], or USER CODE [OFF] AREA [ENTER] to stop the audible alert and cancel the event. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. **Note:** This input type is not used in standard commercial versions of Challenger systems.
18	24-hour local comms fail	In access or secure, an unsealed input generates a local alarm ("Report Fail: Local Alarm" is displayed and the beeper sounds on RASs assigned to the same areas). The Comms Fail LED is activated on applicable RAS models. The local alarm can be reset via RAS by pressing [ENTER] [ENTER] 0 [ENTER], or USER CODE [OFF] AREA [ENTER] to stop the audible alert and cancel the event. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. *Programming*: Local alarm reminder time.
19	Comms fail LED	In access or secure, an unsealed input displays "Report Fail" on RASs assigned to the same area, and the Comms Fail LED is activated on applicable RAS models.

Input type	Name	Description
58	Input to screen text	In access or secure, an unsealed, open, or shorted input displays the system’s event text via LCD RAS. *Example*: Temperature alarm on freezer. *Programming*: Event text. **Note:** This input type cannot indicate tamper.
Camera monitoring—Panel inputs 1 to 16 only (not DGP inputs) that monitor camera film levels. Refer to input types 23, 24, 25, 26, 36, 37, 38, 39, 48, 49, 50, 51, 52, 53, 54, and 55.		
23	Camera 1 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 1. **Note:** This input type cannot indicate tamper.
24	Camera 2 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 2. **Note:** This input type cannot indicate tamper.
25	Camera 3 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 3. **Note:** This input type cannot indicate tamper.
26	Camera 4 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 4. **Note:** This input type cannot indicate tamper.
36	Camera 5 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 5. **Note:** This input type cannot indicate tamper.
37	Camera 6 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 6. **Note:** This input type cannot indicate tamper.
38	Camera 7 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 7. **Note:** This input type cannot indicate tamper.
39	Camera 8 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 8. **Note:** This input type cannot indicate tamper.
48	Camera 1 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 1. **Note:** This input type cannot indicate tamper.
49	Camera 2 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 2. **Note:** This input type cannot indicate tamper.
50	Camera 3 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 3. **Note:** This input type cannot indicate tamper.
51	Camera 4 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 4. **Note:** This input type cannot indicate tamper.

Input type	Name	Description
52	Camera 5 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 5. **Note:** This input type cannot indicate tamper.
53	Camera 6 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 6. **Note:** This input type cannot indicate tamper.
54	Camera 7 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 7. **Note:** This input type cannot indicate tamper.
55	Camera 8 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 8. **Note:** This input type cannot indicate tamper.

Alarm group default settings

Table 29: Challenger user menus and options provided for alarm groups

AG number	Name	Editable?	Challenger user menus and options (defaults)
1	No Access	No	User menus: None Areas: None Option: User Alarm Group
2	Master RAS or Door	No	User menus: All Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress • Reset System Alarms • Remote Access • User Categories: All • Disable auto-deisolate • Auto isolate unsealed inputs • Forced arming • Prevent forced disarming

AG number	Name	Editable?	Challenger user menus and options (defaults)
3	Master Code	No	User menus: All Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress • Reset System Alarms • Remote Access
4 to 10	Spare	No	User menus: None Areas: None Options: None
11	High Level User Master	Yes	User menus: All except 19 Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress • Reset System Alarms • Remote Access
12	Low Level User Master	Yes	User menus: 1, 5, 9, 10, 11, 14, 15, 16 Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress
13	All Area User Code	Yes	User menus: 1, 5, 9, 10, 11 Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress
14	Area 1	Yes	User menus: 1, 5, 9, 10, 11 Area: 1 Options: • Alarm System Control • Keypad Duress
15	Area 2	Yes	User menus: 1, 5, 9, 10, 11 Area: 2 Options: • Alarm System Control • Keypad Duress

AG number	Name	Editable?	Challenger user menus and options (defaults)
16	Area 3	Yes	User menus: 1, 5, 9, 10, 11 Area: 3 Options: • Alarm System Control • Keypad Duress
17	Area 4	Yes	User menus: 1, 5, 9, 10, 11 Area: 4 Options: • Alarm System Control • Keypad Duress
18	Area 5	Yes	User menus: 1, 5, 9, 10, 11 Area: 5 Options: • Alarm System Control • Keypad Duress
19	Area 6	Yes	User menus: 1, 5, 9, 10, 11 Area: 6 Options: • Alarm System Control • Keypad Duress
20	Area 7	Yes	User menus: 1, 5, 9, 10, 11 Area: 7 Options: • Alarm System Control • Keypad Duress
21	Area 8	Yes	User menus: 1, 5, 9, 10, 11 Area: 8 Options: • Alarm System Control • Keypad Duress
22	Area 9	Yes	User menus: 1, 5, 9, 10, 11 Area: 9 Options: • Alarm System Control • Keypad Duress
23	Area 10	Yes	User menus: 1, 5, 9, 10, 11 Area: 10 Options: • Alarm System Control • Keypad Duress

AG number	Name	Editable?	Challenger user menus and options (defaults)
24	Area 11	Yes	User menus: 1, 5, 9, 10, 11 Area: 11 Options: • Alarm System Control • Keypad Duress
25	Area 12	Yes	User menus: 1, 5, 9, 10, 11 Area: 12 Options: • Alarm System Control • Keypad Duress
26	Area 13	Yes	User menus: 1, 5, 9, 10, 11 Area: 13 Options: • Alarm System Control • Keypad Duress
27	Area 14	Yes	User menus: 1, 5, 9, 10, 11 Area: 14 Options: • Alarm System Control • Keypad Duress
28	Area 15	Yes	User menus: 1, 5, 9, 10, 11 Area: 15 Options: • Alarm System Control • Keypad Duress
29	Area 16	Yes	User menus: 1, 5, 9, 10, 11 Area: 16 Options: • Alarm System Control • Keypad Duress
30 to 255	*Program as needed*	Yes	*Program as needed*

Event flags

An event flag is a signal that is activated by a condition in an input, an area, a RAS, a macro, an input shunt, or the system. Event flags can be:

- Predefined (numbered in the range 1 to 16). See Table 30 on page 243.
- Custom (numbered in the range 17 to 255).
- Summary (system event flags, numbered in the range 17 to 255).

Event flags enable the installer to map events to physical relays or to other functions, as required. Event flags may be linked to:

- A relay, see “Option 16: Map relays” on page 165. In the case of relays, you would typically use the relay number as the event flag number.
- A macro, see “Option 35: Program macro logic” on page 187 (a macro can trigger an event flag, which can in turn trigger another macro).
- A shunt timer or a shunt warning timer, see “Option 21: Input shunts” on page 171.

Each event flag can be assigned a name. Refer to “Option 41: Event flag names” on page 200.

Copy the worksheets in “Event flags worksheets” on page 274 to record the details of all user-defined event flags.

An event flag can be used to accomplish more than one task. For example, an event flag can be assigned to an input and to the area containing the input. This enables one event flag to do two things in response to the input’s alarm condition. For example:

- The siren can sound when any of the area’s inputs are in alarm.
- A light can flash above a door (the particular input’s location).

Event flags are programmed in a number of databases, including:

- Input database, see “Option 1: Input database” on page 70 for details.
- Area database, see “Option 2: Area database” on page 77 for details.
- RAS database, see “Option 3: RAS database” on page 83 for details.
- Input shunts, see “Option 21: Input shunts” on page 171 for details.
- System, see “Option 34: Program summary event flags” on page 183 for details.
- Macro logic, see “Option 35: Program macro logic” on page 187 for details.
- DGP database Intelligent Access Controller DGPs can trigger event flags internally. Refer to the DGP’s programming manual for details).

Table 30: Predefined event flags

Number	Functionality	Description
0	Disabled	Use to disable an event flag.
1	Siren	Default siren event flag (assigned in area database). If set to YES in the input database, activates when any siren activates in any area.
2, 3, 4, 5, 9, 10, 11	Secure Alarm	If set to YES on the input database, activates when an alarm is generated by the input and all the areas assigned to the input are secure. It is typically used to activate the system strobe output.

Number	Functionality	Description
6, 7, 13	Access Alarm	If set to YES in the input database, activates when an alarm is generated by the input and one or more of the areas assigned to the input are in access.
8	24-Hour Alarm	If set to YES in the input database, activates at any time an alarm is generated by the input.
16	Tester	Activates during the secure test. A tester event is used to activate a device that allows the testing of other devices. The tester event flag activates for half the tester event flag time programmed in “Option 6: Timers” on page 104. The remaining period of the secure test time is settling time to allow the tested device to switch back to sealed state (make sure that the secure test time is longer than the tester event flag time).

Reporting

A Challenger panel can report (send messages) to a remote monitoring company in a variety of formats.

This section provides details of the following reporting types:

- “CID reporting codes for input events” below
- “CID reporting codes for system events” on page 245
- “STU serial reporting formats” on page 245

Note: Refer to the “Challenger10 ChallengerPlus Event Codes” document for the CID codes and descriptions.

CID reporting codes for input events

For each input that you need to send Ademco Contact ID (CID) event messages to a remote monitoring company, you need to program a report ID type. When selecting report ID types on an LCD RAS, only the Contact ID code and classification are displayed (the sub-classification is not displayed on the RAS).

These CID codes are used for reporting input events:

- From Challenger to the remote monitoring company where the reporting format is Contact ID.
- From a TS2000 Network Master Receiver when receiving events from a Challenger panel where the reporting format is Contact ID.

Note: Refer to the “CID Codes via RAS / Keypad entry” section of the “Challenger10 ChallengerPlus Event Codes” document to view Report Type details and descriptions.

In each case, the area number (01 to 99) is reported in decimal via the group byte.

CID reporting codes for system events

CID codes are used for reporting system events via:

- Challenger panel to a remote monitoring company.
- TS2000 Network Master Receiver when receiving events from a Challenger panel where the reporting format is a Contact ID format or sub-format.

Contact ID formats or sub-formats are used where a communication path’s reporting format is Contact ID Modem, IP Receiver, or a Contact ID sub format of Securitel STU.

Contact ID messages typically contain only decimal values, except where a Contact ID Hex sub-format is specified. In Contact ID Hex reporting the CID message’s group number and point ID are offset by 2000 and reported in “hex” to a monitoring station (hex format in this instance is based on Ademco Contact ID Protocol (0 to 9 and B to F).

Note: Refer to the “Decimal to CID Hex cross-reference” section of the “Challenger10 ChallengerPlus Event Codes” document to view a conversion table showing Contact ID Hex values used in the Challenger system.

STU serial reporting formats

The hex values in this section are true hexadecimal (base 16) and not the CID hex (0-9, B-F).

Note: Refer to the “STU serial reporting formats” section of the “Challenger10 ChallengerPlus Event Codes” document to view STU reporting codes used in the Challenger system.

Programming map

The Challenger menu is divided into two main functional areas:

- User menu (see “User menu structure” on page 14).
- Install menu (see Figure 27 on page 246, Figure 28 on page 247, and Figure 29 on page 248).

The Install menus depicted on the following pages display unrestricted user access and contain options that do not apply to every Challenger system.

Access to the Install menu is typically limited to trained Challenger system installers and other service technicians to program the Challenger system. Some of the options contained in the Install menu can adversely affect the operation of the system if used incorrectly.

Figure 27: Install menu structure (options 1 to 10)

Install menu option	Summary
1-Input database	Input number • name • type • report ID • area, area group, or alarm group • test option • event flags • test within days • second event flag • second event flag triggers
2-Area database	Area number • name • entry and exit times • area account • event flags • out-of-hours time zone • disarm time • perimeter area
3-RAS database	Poll RAS • RAS number • area and menu alarm groups • door event flag • relay number • LCD arming station • toggle keyboard control • ENTER key opens door only • door event flag on alarm codes • display shunting on LCD • disarm/arm using one key • cards auto disarm • cards always disarm/arm • reset from RAS without code • restrict user category to disarm • cards arm after three badges • card and code • entry and exit console warning • area LED assignment
4-DGP database	Poll DGP • DGP address • DGP type
5-Alarm groups	Alarm group number • name • area or area group • user alarm group • alarm system control • prompt with list of areas • keypad duress • reset system alarms • can area be armed • can area be disarmed • can area be reset • can area be timed • disable auto-deisolate • auto isolate unsealed inputs • forced arming when inputs unsealed • prevent forced disarming • can user access via remote • user categories • no arming if user category not timing • enable area search • user menu options • time • alternate alarm group
6-Timers	User category • access test • secure test • warning • delay holdup • suspicion • service • local alarm reminder • individual input test • doors unlock • tester event flag • siren • mains fail • card to code • min area search • max area search • max twin trip
7-System options	Total disarm area or area group • film low and out levels • test mode • relay controllers • event text • alarm code prefix value • LCD text rotation time and speed • input tamper monitoring • auto deisolate • display one input at a time • user name • system alarms set siren and strobe • latching system alarms • siren testing • disable 0 ENTER for camera reset • disable insert of user category • disable code from displaying • disable flashing area LEDs • dual custody programming • display alarms instantly on LCD • sirens only after report fail • financial institution options • display user flags • delayed holdup lockout • skip access check for service tech • expanded test reporting • expanded test success reporting • exit fault reporting • enable V8 multibreak • enable V8 numbering • EOL resistor • time zone • area search time zone • card learn RAS • decrement test days during TZ • external and internal siren modes
8-Auto reset	Auto reset time • alarm group
9-Communications	**Set up hardware:** • monitor ring • blind dial • PSTN line fault monitor • baud rate • parity • stop bits • USB options • enable Ethernet • enable ping • IP address • subnet mask • gateway address • DNS addresses • WiFi options • GSM options **Set up path:** • path number • format • enable path • path name • location • slot • account code • priority • backup path • computer password • always connect • connect on event • connect on service • connect on buffer at 80% • isolated inputs trigger path • stay connected on empty buffer • control command • trigger comms fail event • area account codes • heartbeat fail triggers path • filter event to area • event time zone • multibreak alarm timer • report alarm events • report access events • send events out of TZ • remove unsent events • system alarm report • multibreak alarms • multibreak restores • report open/close • common open/close • report computer connected • test calls • PABX number • first and second telephone numbers • number of redials • number of calls to answer • number of rings to answer • auto answer • call back • DTMF dial • send to IP address • send and listen IP ports • IP mode • dynamic IP address • encryption type • encryption keys • computer attempts • message ACK timeout • message retries • connect timeout • connect retries • wait time between connections • heartbeat timeout **Status:** • path status • hardware status • management software **UltraSync:** • setup • reports • status • auto setup
10-Reserved	Not used in this version

Continued on next page ...

Figure 28: Install menu structure (options 11 to 31)

Install menu option	Summary
11-Version	Check the type and version of the panel, a RAS, or a DGP
12-Lamp test	Turn on RAS LEDs
13-Timezones	Program the panel’s hard time zones
14-Defaults	Reset the panel to default settings, or clear the history buffer
15-User category	User category number and name
16-Map relays	Relay number • event flag • time zone • active or inactive during time zone • invert relay
17-Arm/disarm via Tz	Arm/disarm time program number • time zone to arm/disarm • alarm group to auto arm/disarm
18-Vaults	Program an area or area group as a vault to be controlled by other areas
19-Area linking	Use area linking to create inputs in a common area
20-Reserved	Not used in this version
21-Input shunts	Shunt timer number • input number to shunt • relay number to start shunt • shunt time • shunt warning time • shunt event flag • shunt warning event flag • shunt RAS • door open command starts shunt • door shunted in access • door shunted in secure • cancel door event flag • input holds event flag at 2 seconds • entry/exit shunting • report door open/close
22-TZ to follow relays	Select (soft) time zone • assign relay to time zone
23-Poll errors	Select device type • select device number
24-Send Programming	Display the send operation status • select item to send (users, door and floor groups, time zones, holidays)
25-Display last card	Display the RAS number and card data of the last card read
26-Diagnostics	Skip this option. It is reserved for factory use
27-Reserved	Not used in this version
28-Remote controllers	Select device type and number to access remote device programming
29-Panel voltage & current	View details of the panel’s power use
30-Reserved	Not used in this version
31-Battery testing	Select battery test program • program automatic battery test frequency, start time and period • perform manual battery test • manual battery test report • select DGP or panel for manual battery test • manual battery test period

Continued on next page ...

Figure 29: Install menu structure (options 32 to 45)

Install menu option	Summary
32-Custom message	Create a custom message for the RAS's initial LCD screen
33-Program next service	Program the next maintenance date and RAS message
34-Program summary event flags	Mains fail • low battery • fuse fail • tamper • siren fail • DGP isolate • DGP offline • RAS offline • duress • film out • report fail • test mode • all secured • console trigger • area search running • area search done
35-Program macro logic	Macro number • output function • output time • output triggers event flag or input • inputs • logic equation
36-Area groups	Organise the 99 areas into groups for easier control
37-SD card backup/restore	Backup • restore • status
38-Reset input test days	Set the days to 0 for timed input testing
39-Automation	Automation zone number • name • enable zone • event flag to trigger zone • invert trigger • time zone to disable trigger • time zone to trigger zone • when zone triggered set level to • when zone reset set level to • when triggered zone on for • ramp rate • enable logging • enable quick control • enable manual control • manual on control • manual off control • control zone on RAS • zone activates event flag • set event flag at level • reset event flag at level • zone type • group number • network number • app number
40-Door/lift names and E/F trigger	Door number • name • door event flag • time to trigger
41-Event flag names	Event flag number • name
42-Challenger name	Name
43-Automation status	Automation zone number • activate • on • off
44-Standard lifts	Lift number Enable **Lift settings:** • name • remote reader • lift access time • remote reader access time • override floor group • security floor group • security trigger event flag • floor relays **Delete lift**
45-Standard doors	Door number Enable **Door access option:** • name • access time • pre lock time • post lock time • override timezone • override after entry • Report door DOTL • Report door FORCED • Report door open/close • Report door secured/unsecured **Shunting/Passback/Egress:** • shunting • shunt time • warning time • cancel shunt when door closes • egress timezone • egress reporting **Alarm control:** • alarm group • alarm control • multi badge time • denied if area secured **Hardware:** • lock type • door input 1 • egress input • DOTL input • lock relay • warning relay **Delete door**

Appendix B
Programming worksheets

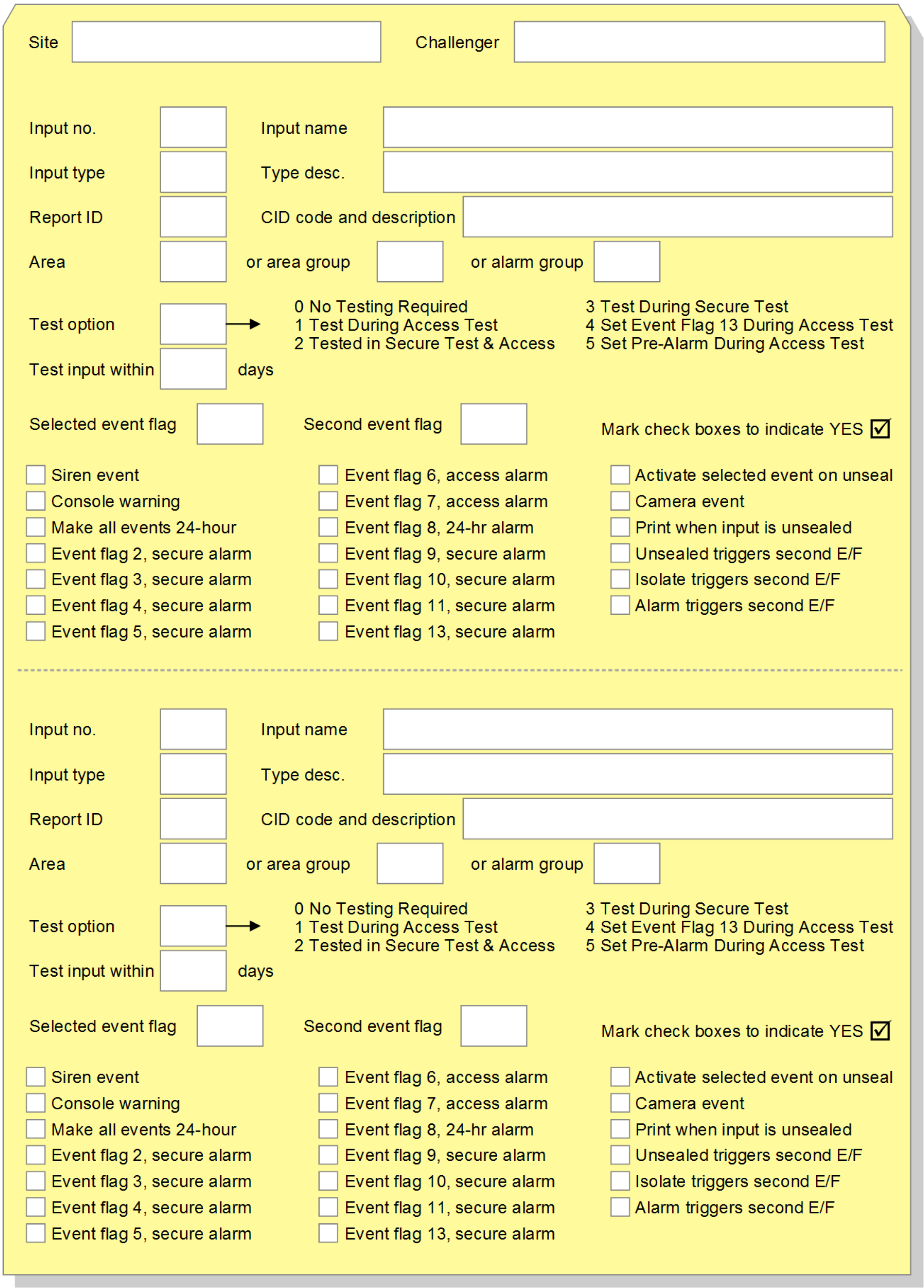
Print these worksheets as needed to record the system's programming details.

Content

Input worksheet

For programming details see “Option 1: Input database” on page 70.

Figure 30: Input worksheet



Site ________ Challenger ________

Input no. ____ Input name ________

Input type ____ Type desc. ________

Report ID ____ CID code and description ________

Area ____ or area group ____ or alarm group ____

Test option ____ →

0 No Testing Required
1 Test During Access Test
2 Tested in Secure Test & Access
3 Test During Secure Test
4 Set Event Flag 13 During Access Test
5 Set Pre-Alarm During Access Test

Test input within ____ days

Selected event flag ____ Second event flag ____

Mark check boxes to indicate YES ☑

- □ Siren event
- □ Console warning
- □ Make all events 24-hour
- □ Event flag 2, secure alarm
- □ Event flag 3, secure alarm
- □ Event flag 4, secure alarm
- □ Event flag 5, secure alarm
- □ Event flag 6, access alarm
- □ Event flag 7, access alarm
- □ Event flag 8, 24-hr alarm
- □ Event flag 9, secure alarm
- □ Event flag 10, secure alarm
- □ Event flag 11, secure alarm
- □ Event flag 13, secure alarm
- □ Activate selected event on unseal
- □ Camera event
- □ Print when input is unsealed
- □ Unsealed triggers second E/F
- □ Isolate triggers second E/F
- □ Alarm triggers second E/F

Input no. ____ Input name ________

Input type ____ Type desc. ________

Report ID ____ CID code and description ________

Area ____ or area group ____ or alarm group ____

Test option ____ →

0 No Testing Required
1 Test During Access Test
2 Tested in Secure Test & Access
3 Test During Secure Test
4 Set Event Flag 13 During Access Test
5 Set Pre-Alarm During Access Test

Test input within ____ days

Selected event flag ____ Second event flag ____

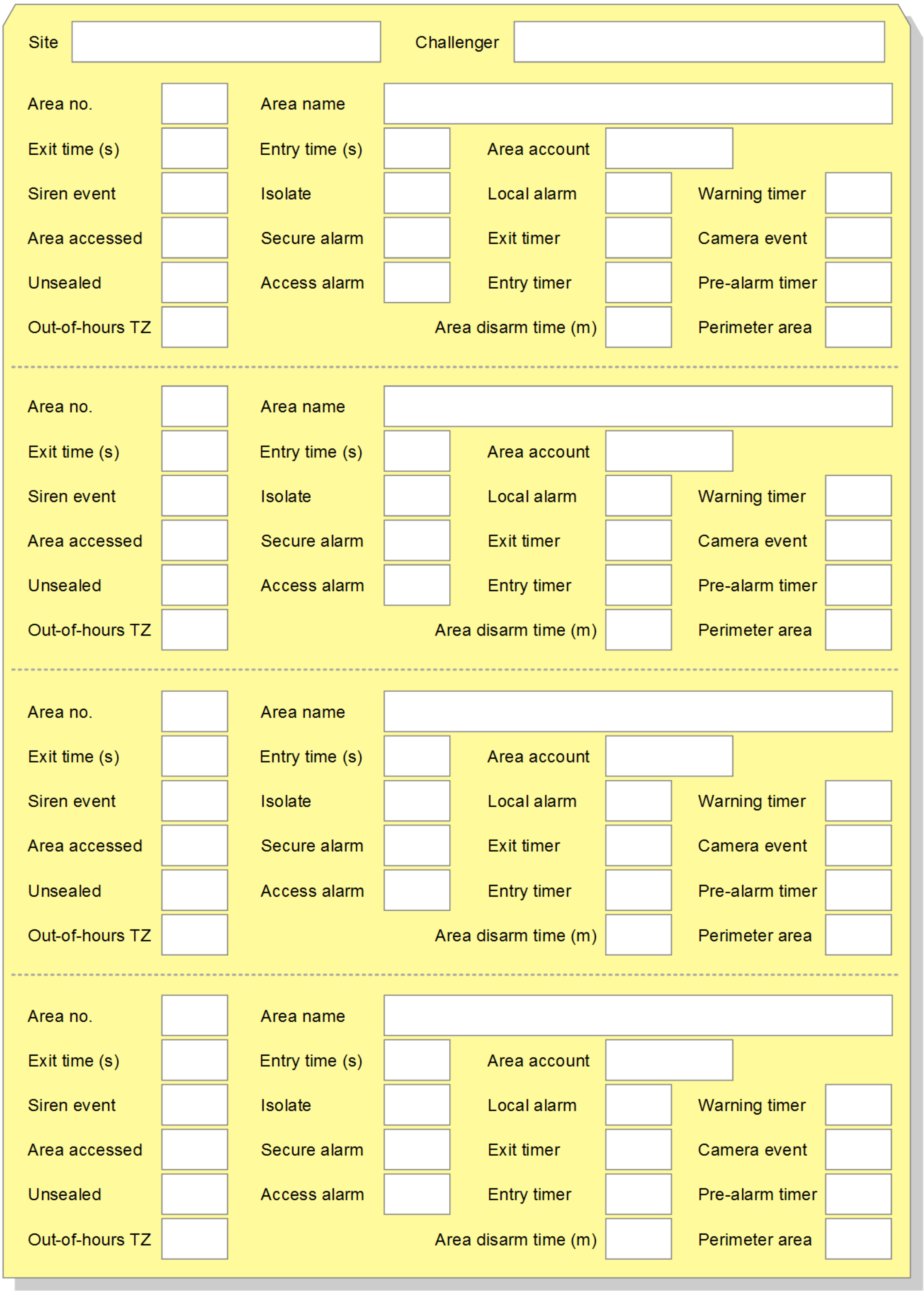
Mark check boxes to indicate YES ☑

- □ Siren event
- □ Console warning
- □ Make all events 24-hour
- □ Event flag 2, secure alarm
- □ Event flag 3, secure alarm
- □ Event flag 4, secure alarm
- □ Event flag 5, secure alarm
- □ Event flag 6, access alarm
- □ Event flag 7, access alarm
- □ Event flag 8, 24-hr alarm
- □ Event flag 9, secure alarm
- □ Event flag 10, secure alarm
- □ Event flag 11, secure alarm
- □ Event flag 13, secure alarm
- □ Activate selected event on unseal
- □ Camera event
- □ Print when input is unsealed
- □ Unsealed triggers second E/F
- □ Isolate triggers second E/F
- □ Alarm triggers second E/F

Area worksheet

For programming details see “Option 2: Area database” on page 77.

Figure 31: Area worksheet



Site		Challenger	

Area no.		Area name					
Exit time (s)		Entry time (s)		Area account			
Siren event		Isolate		Local alarm		Warning timer	
Area accessed		Secure alarm		Exit timer		Camera event	
Unsealed		Access alarm		Entry timer		Pre-alarm timer	
Out-of-hours TZ				Area disarm time (m)		Perimeter area	

Area no.		Area name					
Exit time (s)		Entry time (s)		Area account			
Siren event		Isolate		Local alarm		Warning timer	
Area accessed		Secure alarm		Exit timer		Camera event	
Unsealed		Access alarm		Entry timer		Pre-alarm timer	
Out-of-hours TZ				Area disarm time (m)		Perimeter area	

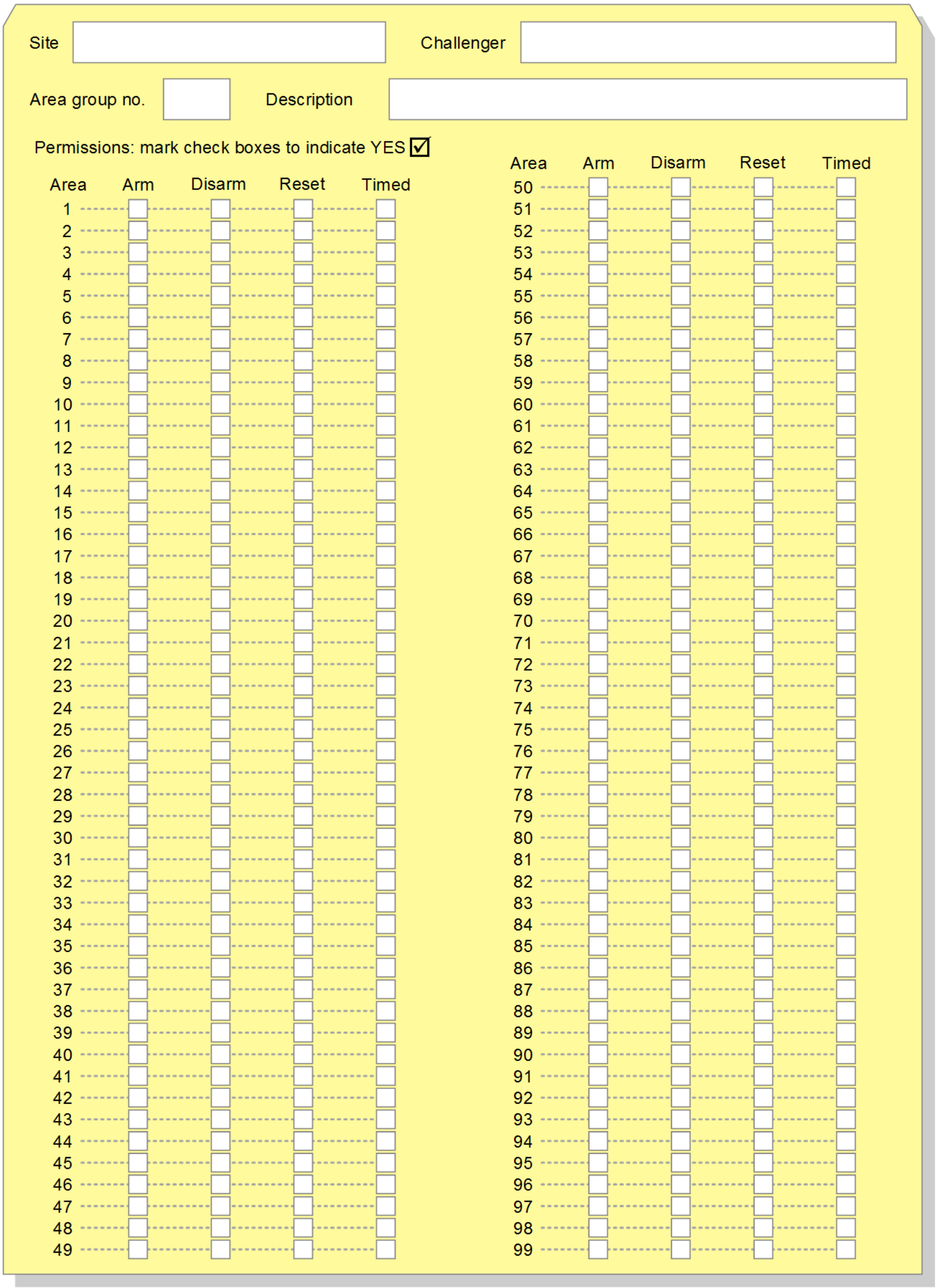
Area no.		Area name					
Exit time (s)		Entry time (s)		Area account			
Siren event		Isolate		Local alarm		Warning timer	
Area accessed		Secure alarm		Exit timer		Camera event	
Unsealed		Access alarm		Entry timer		Pre-alarm timer	
Out-of-hours TZ				Area disarm time (m)		Perimeter area	

Area no.		Area name					
Exit time (s)		Entry time (s)		Area account			
Siren event		Isolate		Local alarm		Warning timer	
Area accessed		Secure alarm		Exit timer		Camera event	
Unsealed		Access alarm		Entry timer		Pre-alarm timer	
Out-of-hours TZ				Area disarm time (m)		Perimeter area	

Area group worksheet

For programming details see “Option 36: Area groups” on page 190.

Figure 32: Area group worksheet



Site □ Challenger □

Area group no. □ Description □

Permissions: mark check boxes to indicate YES ☑

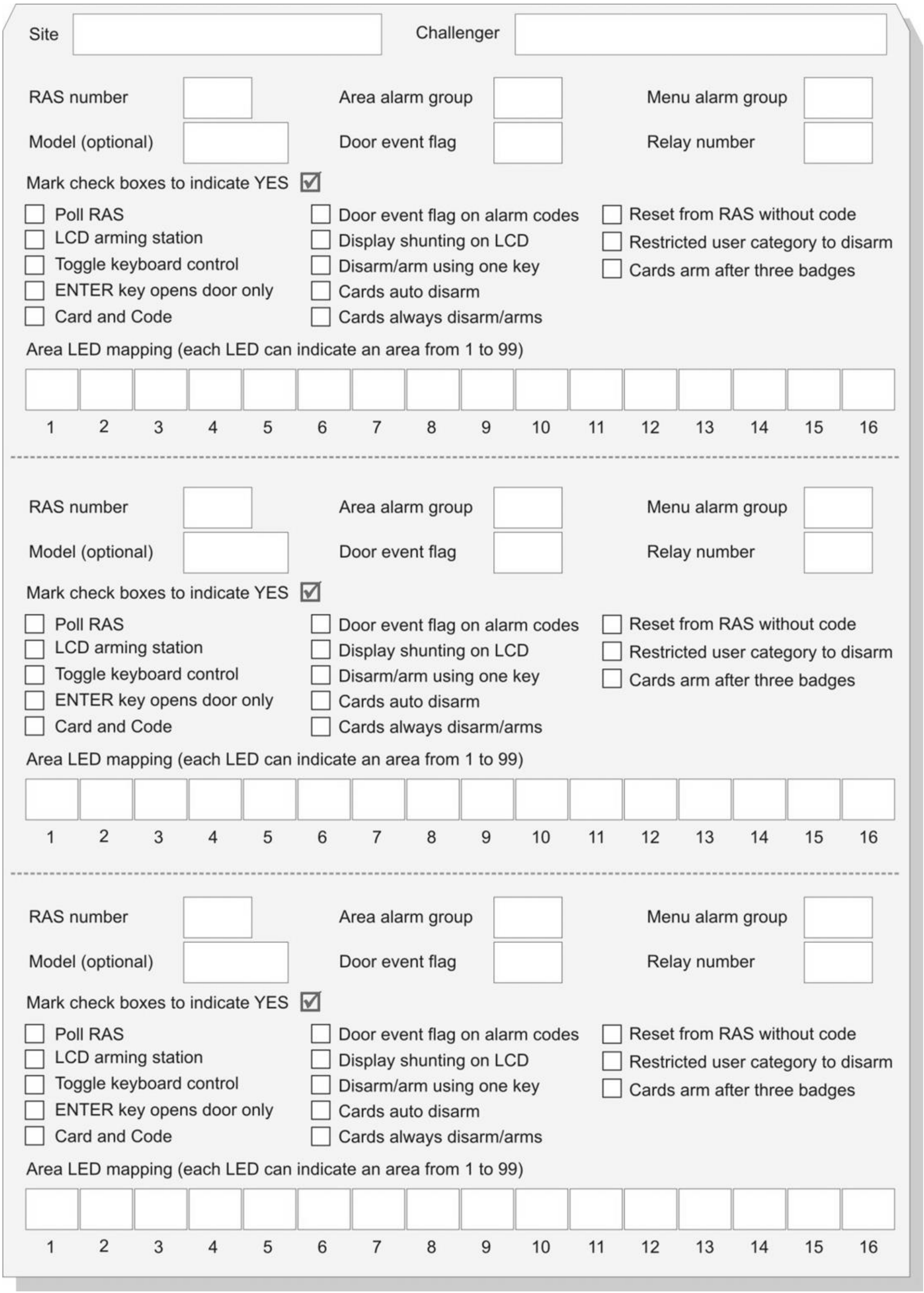
Area	Arm	Disarm	Reset	Timed
1	□	□	□	□
2	□	□	□	□
3	□	□	□	□
4	□	□	□	□
5	□	□	□	□
6	□	□	□	□
7	□	□	□	□
8	□	□	□	□
9	□	□	□	□
10	□	□	□	□
11	□	□	□	□
12	□	□	□	□
13	□	□	□	□
14	□	□	□	□
15	□	□	□	□
16	□	□	□	□
17	□	□	□	□
18	□	□	□	□
19	□	□	□	□
20	□	□	□	□
21	□	□	□	□
22	□	□	□	□
23	□	□	□	□
24	□	□	□	□
25	□	□	□	□
26	□	□	□	□
27	□	□	□	□
28	□	□	□	□
29	□	□	□	□
30	□	□	□	□
31	□	□	□	□
32	□	□	□	□
33	□	□	□	□
34	□	□	□	□
35	□	□	□	□
36	□	□	□	□
37	□	□	□	□
38	□	□	□	□
39	□	□	□	□
40	□	□	□	□
41	□	□	□	□
42	□	□	□	□
43	□	□	□	□
44	□	□	□	□
45	□	□	□	□
46	□	□	□	□
47	□	□	□	□
48	□	□	□	□
49	□	□	□	□

Area	Arm	Disarm	Reset	Timed
50	□	□	□	□
51	□	□	□	□
52	□	□	□	□
53	□	□	□	□
54	□	□	□	□
55	□	□	□	□
56	□	□	□	□
57	□	□	□	□
58	□	□	□	□
59	□	□	□	□
60	□	□	□	□
61	□	□	□	□
62	□	□	□	□
63	□	□	□	□
64	□	□	□	□
65	□	□	□	□
66	□	□	□	□
67	□	□	□	□
68	□	□	□	□
69	□	□	□	□
70	□	□	□	□
71	□	□	□	□
72	□	□	□	□
73	□	□	□	□
74	□	□	□	□
75	□	□	□	□
76	□	□	□	□
77	□	□	□	□
78	□	□	□	□
79	□	□	□	□
80	□	□	□	□
81	□	□	□	□
82	□	□	□	□
83	□	□	□	□
84	□	□	□	□
85	□	□	□	□
86	□	□	□	□
87	□	□	□	□
88	□	□	□	□
89	□	□	□	□
90	□	□	□	□
91	□	□	□	□
92	□	□	□	□
93	□	□	□	□
94	□	□	□	□
95	□	□	□	□
96	□	□	□	□
97	□	□	□	□
98	□	□	□	□
99	□	□	□	□

RAS worksheet

For programming details see “Option 3: RAS database” on page 83.

Figure 33: RAS worksheet



Site

Challenger

RAS number

Area alarm group

Menu alarm group

Model (optional)

Door event flag

Relay number

Mark check boxes to indicate YES ☑

□ Poll RAS
□ LCD arming station
□ Toggle keyboard control
□ ENTER key opens door only
□ Card and Code

□ Door event flag on alarm codes
□ Display shunting on LCD
□ Disarm/arm using one key
□ Cards auto disarm
□ Cards always disarm/arms

□ Reset from RAS without code
□ Restricted user category to disarm
□ Cards arm after three badges

Area LED mapping (each LED can indicate an area from 1 to 99)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

RAS number

Area alarm group

Menu alarm group

Model (optional)

Door event flag

Relay number

Mark check boxes to indicate YES ☑

□ Poll RAS
□ LCD arming station
□ Toggle keyboard control
□ ENTER key opens door only
□ Card and Code

□ Door event flag on alarm codes
□ Display shunting on LCD
□ Disarm/arm using one key
□ Cards auto disarm
□ Cards always disarm/arms

□ Reset from RAS without code
□ Restricted user category to disarm
□ Cards arm after three badges

Area LED mapping (each LED can indicate an area from 1 to 99)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

RAS number

Area alarm group

Menu alarm group

Model (optional)

Door event flag

Relay number

Mark check boxes to indicate YES ☑

□ Poll RAS
□ LCD arming station
□ Toggle keyboard control
□ ENTER key opens door only
□ Card and Code

□ Door event flag on alarm codes
□ Display shunting on LCD
□ Disarm/arm using one key
□ Cards auto disarm
□ Cards always disarm/arms

□ Reset from RAS without code
□ Restricted user category to disarm
□ Cards arm after three badges

Area LED mapping (each LED can indicate an area from 1 to 99)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Site ☐ Challenger ☐

RAS number ☐ RAS name ☐

Area alarm group ☐ Door event flag ☐ Model (optional) ☐

Menu alarm group ☐ Relay number ☐

Mark check boxes to indicate YES ☑

□ Poll RAS
□ LCD arming station
□ Toggle keyboard control
□ ENTER key opens door only
□ Door event flag on alarm codes
□ Display shunting on LCD
□ Disarm/arm using one key
□ Cards auto disarm
□ Cards always disarm/arms
□ Reset from RAS without code
□ Restricted user category to disarm
□ Cards arm after three badges
□ Card and code
□ Entry and exit console warning

Area LED mapping (each LED can indicate an area from 1 to 99)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

RAS number ☐ RAS name ☐

Area alarm group ☐ Door event flag ☐ Model (optional) ☐

Menu alarm group ☐ Relay number ☐

Mark check boxes to indicate YES ☑

□ Poll RAS
□ LCD arming station
□ Toggle keyboard control
□ ENTER key opens door only
□ Door event flag on alarm codes
□ Display shunting on LCD
□ Disarm/arm using one key
□ Cards auto disarm
□ Cards always disarm/arms
□ Reset from RAS without code
□ Restricted user category to disarm
□ Cards arm after three badges
□ Card and code
□ Entry and exit console warning

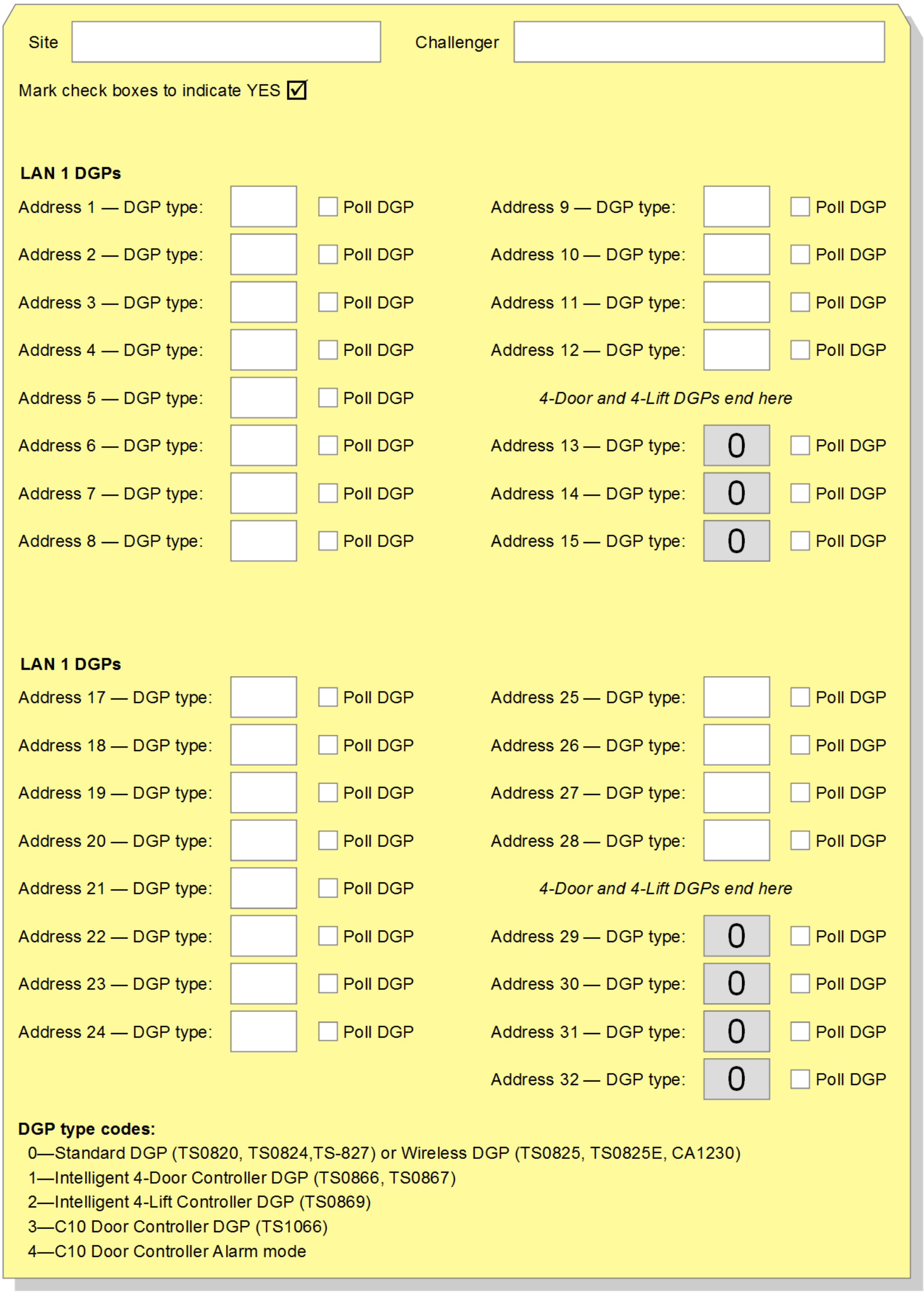
Area LED mapping (each LED can indicate an area from 1 to 99)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

DGPs worksheet

For programming details see “Option 4: DGP database” on page 93.

Figure 34: DGP worksheet



Site ______ Challenger ______

Mark check boxes to indicate YES ☑

LAN 1 DGPs

Address 1 — DGP type:		□ Poll DGP	Address 9 — DGP type:		□ Poll DGP
Address 2 — DGP type:		□ Poll DGP	Address 10 — DGP type:		□ Poll DGP
Address 3 — DGP type:		□ Poll DGP	Address 11 — DGP type:		□ Poll DGP
Address 4 — DGP type:		□ Poll DGP	Address 12 — DGP type:		□ Poll DGP
Address 5 — DGP type:		□ Poll DGP	*4-Door and 4-Lift DGPs end here*		
Address 6 — DGP type:		□ Poll DGP	Address 13 — DGP type:	0	□ Poll DGP
Address 7 — DGP type:		□ Poll DGP	Address 14 — DGP type:	0	□ Poll DGP
Address 8 — DGP type:		□ Poll DGP	Address 15 — DGP type:	0	□ Poll DGP

LAN 1 DGPs

Address 17 — DGP type:		□ Poll DGP	Address 25 — DGP type:		□ Poll DGP
Address 18 — DGP type:		□ Poll DGP	Address 26 — DGP type:		□ Poll DGP
Address 19 — DGP type:		□ Poll DGP	Address 27 — DGP type:		□ Poll DGP
Address 20 — DGP type:		□ Poll DGP	Address 28 — DGP type:		□ Poll DGP
Address 21 — DGP type:		□ Poll DGP	*4-Door and 4-Lift DGPs end here*		
Address 22 — DGP type:		□ Poll DGP	Address 29 — DGP type:	0	□ Poll DGP
Address 23 — DGP type:		□ Poll DGP	Address 30 — DGP type:	0	□ Poll DGP
Address 24 — DGP type:		□ Poll DGP	Address 31 — DGP type:	0	□ Poll DGP
			Address 32 — DGP type:	0	□ Poll DGP

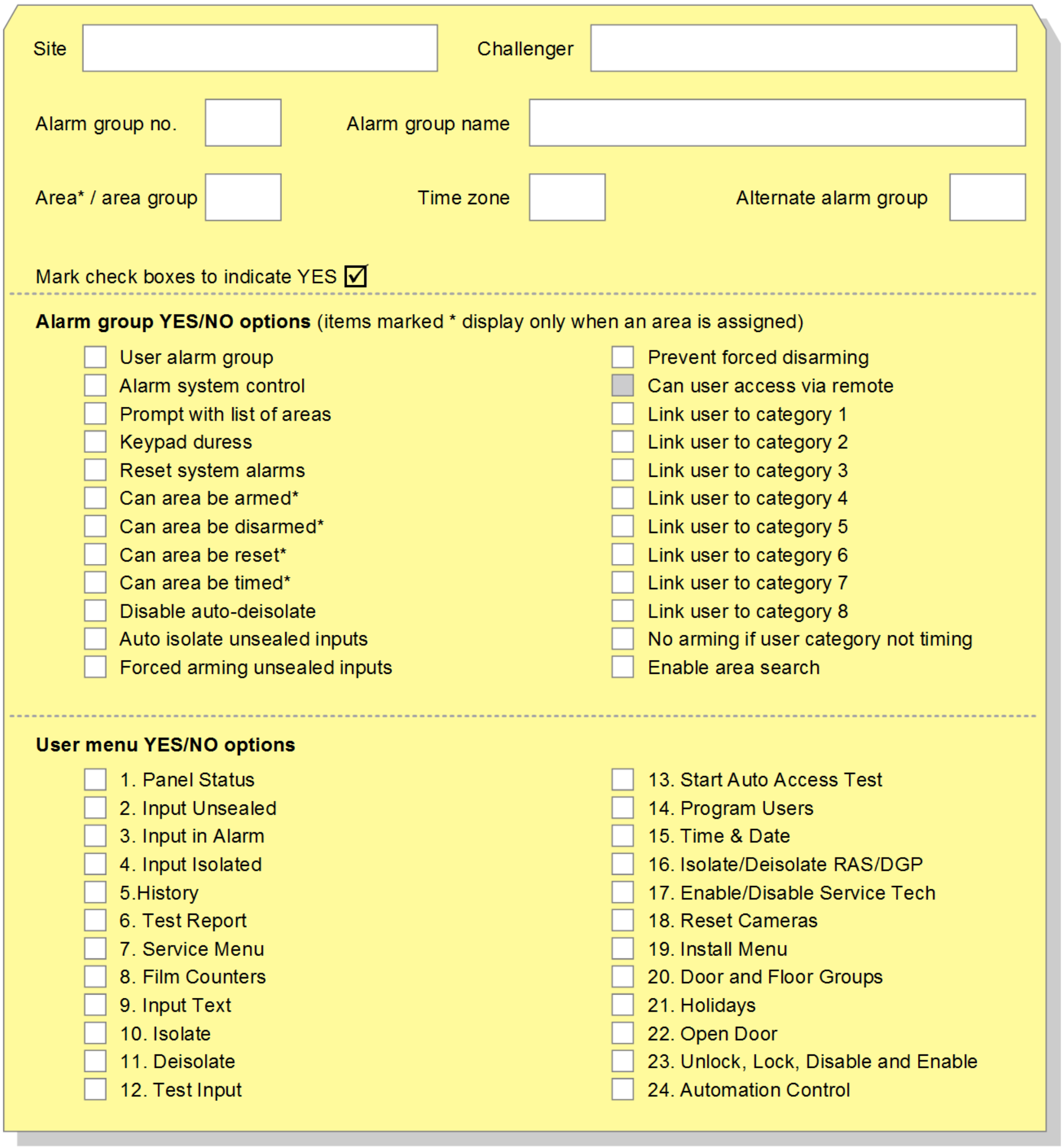
DGP type codes:

0—Standard DGP (TS0820, TS0824,TS-827) or Wireless DGP (TS0825, TS0825E, CA1230)
1—Intelligent 4-Door Controller DGP (TS0866, TS0867)
2—Intelligent 4-Lift Controller DGP (TS0869)
3—C10 Door Controller DGP (TS1066)
4—C10 Door Controller Alarm mode

Alarm group worksheet

For programming details see “Option 5: Alarm groups” on page 96.

Figure 35: Alarm Group worksheet



Site ______ Challenger ______

Alarm group no. ______ Alarm group name ______

Area* / area group ______ Time zone ______ Alternate alarm group ______

Mark check boxes to indicate YES ☑

Alarm group YES/NO options (items marked * display only when an area is assigned)

□ User alarm group
□ Alarm system control
□ Prompt with list of areas
□ Keypad duress
□ Reset system alarms
□ Can area be armed*
□ Can area be disarmed*
□ Can area be reset*
□ Can area be timed*
□ Disable auto-deisolate
□ Auto isolate unsealed inputs
□ Forced arming unsealed inputs

□ Prevent forced disarming
▨ Can user access via remote
□ Link user to category 1
□ Link user to category 2
□ Link user to category 3
□ Link user to category 4
□ Link user to category 5
□ Link user to category 6
□ Link user to category 7
□ Link user to category 8
□ No arming if user category not timing
□ Enable area search

User menu YES/NO options

□ 1. Panel Status
□ 2. Input Unsealed
□ 3. Input in Alarm
□ 4. Input Isolated
□ 5.History
□ 6. Test Report
□ 7. Service Menu
□ 8. Film Counters
□ 9. Input Text
□ 10. Isolate
□ 11. Deisolate
□ 12. Test Input

□ 13. Start Auto Access Test
□ 14. Program Users
□ 15. Time & Date
□ 16. Isolate/Deisolate RAS/DGP
□ 17. Enable/Disable Service Tech
□ 18. Reset Cameras
□ 19. Install Menu
□ 20. Door and Floor Groups
□ 21. Holidays
□ 22. Open Door
□ 23. Unlock, Lock, Disable and Enable
□ 24. Automation Control

Timers worksheet

For programming details see “Option 6: Timers” on page 104.

Figure 36: Timers worksheet

Site		Challenger	

User category 1 (m)		User category 8 (m)		Local alarm reminder (m)	
User category 2 (m)		Access test (m)		Individual testmode (m)	
User category 3 (m)		Secure test (m)		Door(s) unlock (s)	
User category 4 (m)		Warning (m)		Tester event flag (s)	
User category 5 (m)		Delay holdup (s)		Siren (m)	
User category 6 (m)		Suspicion (s)		Mains fail (m)	
User category 7 (m)		Service (m)		Card to code (s)	
Min area search (m)		Max area search (m)			

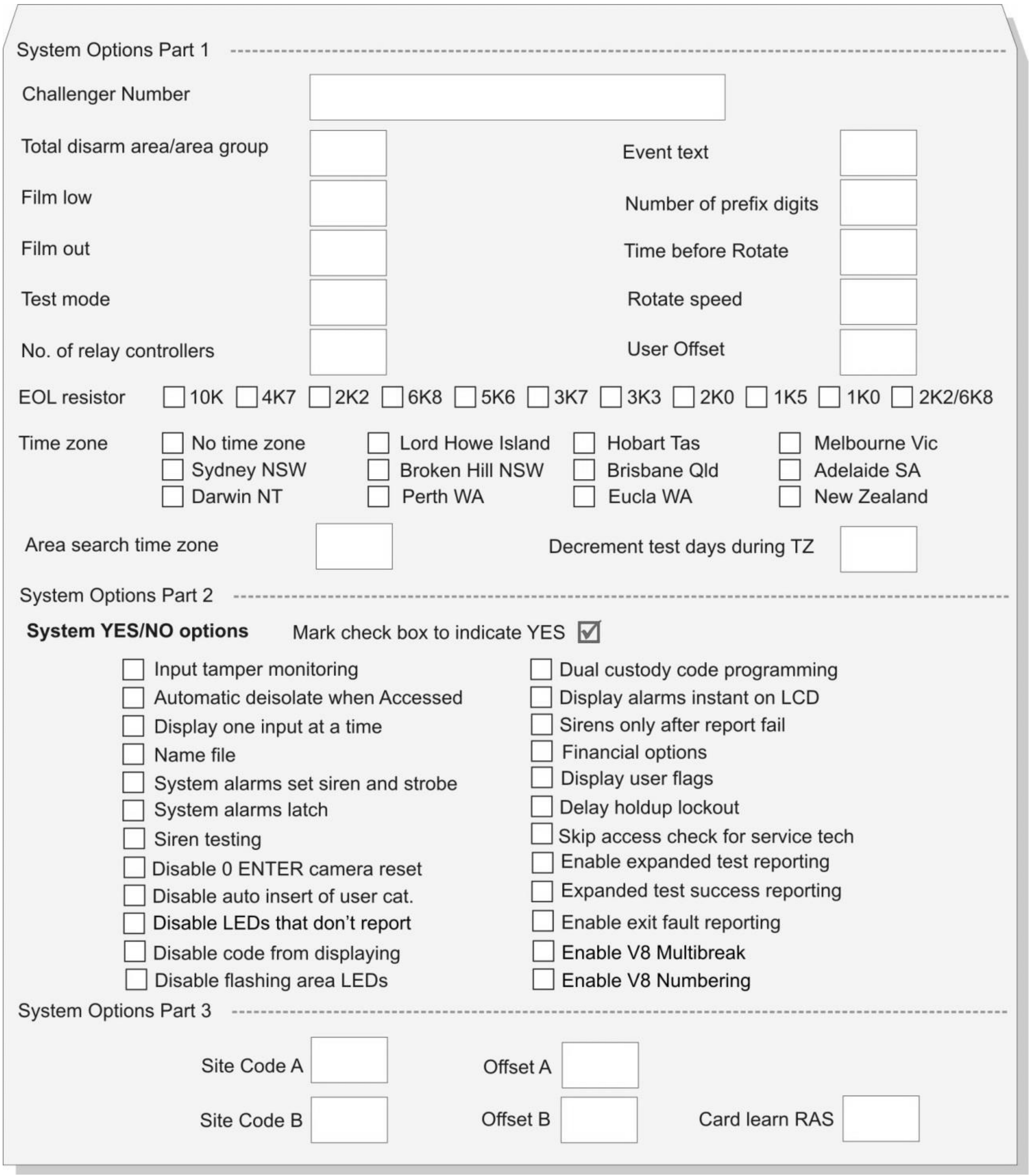
Site		Challenger	

User category 1 (m)		Access test (m)		Door(s) unlock (s)	
User category 2 (m)		Secure test (m)		Tester event flag (s)	
User category 3 (m)		Warning (m)		Siren (m)	
User category 4 (m)		Delay holdup (s)		Mains fail (m)	
User category 5 (m)		Suspicion (s)		Card to code (s)	
User category 6 (m)		Service (m)		Min area search time (m)	
User category 7 (m)		Local alarm reminder (m)		Max area search time (m)	
User category 8 (m)		Individual input test (m)		Max twin trip (s)	

System options worksheet

For programming details see “Option 7: System options” on page 108.

Figure 37: System options worksheet



System Options Part 1

Challenger Number	□		
Total disarm area/area group	□	Event text	□
Film low	□	Number of prefix digits	□
Film out	□	Time before Rotate	□
Test mode	□	Rotate speed	□
No. of relay controllers	□	User Offset	□

EOL resistor □ 10K □ 4K7 □ 2K2 □ 6K8 □ 5K6 □ 3K7 □ 3K3 □ 2K0 □ 1K5 □ 1K0 □ 2K2/6K8

Time zone

□ No time zone	□ Lord Howe Island	□ Hobart Tas	□ Melbourne Vic
□ Sydney NSW	□ Broken Hill NSW	□ Brisbane Qld	□ Adelaide SA
□ Darwin NT	□ Perth WA	□ Eucla WA	□ New Zealand

Area search time zone □ Decrement test days during TZ □

System Options Part 2

System YES/NO options Mark check box to indicate YES ☑

- □ Input tamper monitoring
- □ Automatic deisolate when Accessed
- □ Display one input at a time
- □ Name file
- □ System alarms set siren and strobe
- □ System alarms latch
- □ Siren testing
- □ Disable 0 ENTER camera reset
- □ Disable auto insert of user cat.
- □ Disable LEDs that don’t report
- □ Disable code from displaying
- □ Disable flashing area LEDs
- □ Dual custody code programming
- □ Display alarms instant on LCD
- □ Sirens only after report fail
- □ Financial options
- □ Display user flags
- □ Delay holdup lockout
- □ Skip access check for service tech
- □ Enable expanded test reporting
- □ Expanded test success reporting
- □ Enable exit fault reporting
- □ Enable V8 Multibreak
- □ Enable V8 Numbering

System Options Part 3

Site Code A	□	Offset A	□		
Site Code B	□	Offset B	□	Card learn RAS	□

Site		Challenger	

System Options Part 1

Total disarm area/area group		Event text	
Film low		Number of prefix digits	
Film out		Time before rotate	
Test mode		Rotate speed	
No. of relay controllers		User offset	

EOL resistor □ 10K □ 4K7 □ 2K2 □ 6K8 □ 6K6 □ 3K7 □ 3K3 □ 2K0 □ 1K5 □ 1K0 □ 2K2/6K8

Time zone
- □ No time zone
- □ Sydney NSW
- □ Darwin NT
- □ Lord Howe Island
- □ Broken Hill NSW
- □ Perth WA
- □ Hobart Tas
- □ Brisbane Qld
- □ Eucla WA
- □ Melbourne Vic
- □ Adelaide SA
- □ New Zealand

Area search time zone		Decrement test days during TZ	

System Options Part 2

System YES/NO options Mark check boxes to indicate YES ☑

- □ Input tamper monitoring
- □ Automatic deisolate when accessed
- □ Display one input at a time
- □ Name file
- □ System alarms set siren and strobe
- □ System alarms latch
- □ Siren testing
- □ Disable 0 ENTER camera reset
- □ Disable auto insert of user category
- □ Disable LEDs that don’t report
- □ Disable code from displaying
- □ Disable flashing area LEDs
- □ Dual custody code programming
- □ Display alarms instant on LCD
- □ Sirens only after report fail
- □ Financial options
- □ Display user flags
- □ Delay holdup lockout
- □ Skip access check for service tech
- □ Enable expanded test reporting
- □ Expanded test success reporting
- □ Enable exit fault recording
- □ Enable V8 multibreak
- □ Enable V8 numbering

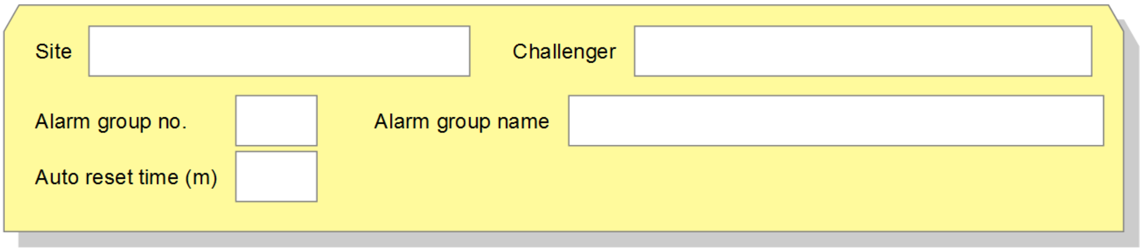
System Options Part 3

Site Code A		Card learn RAS	
Offset A		External siren mode	
Site Code B		Internal siren mode	
Offset B			

Auto reset worksheet

For programming details see “Option 8: Auto reset” on page 121.

Figure 38: Auto reset worksheet



Site

Challenger

Alarm group no.

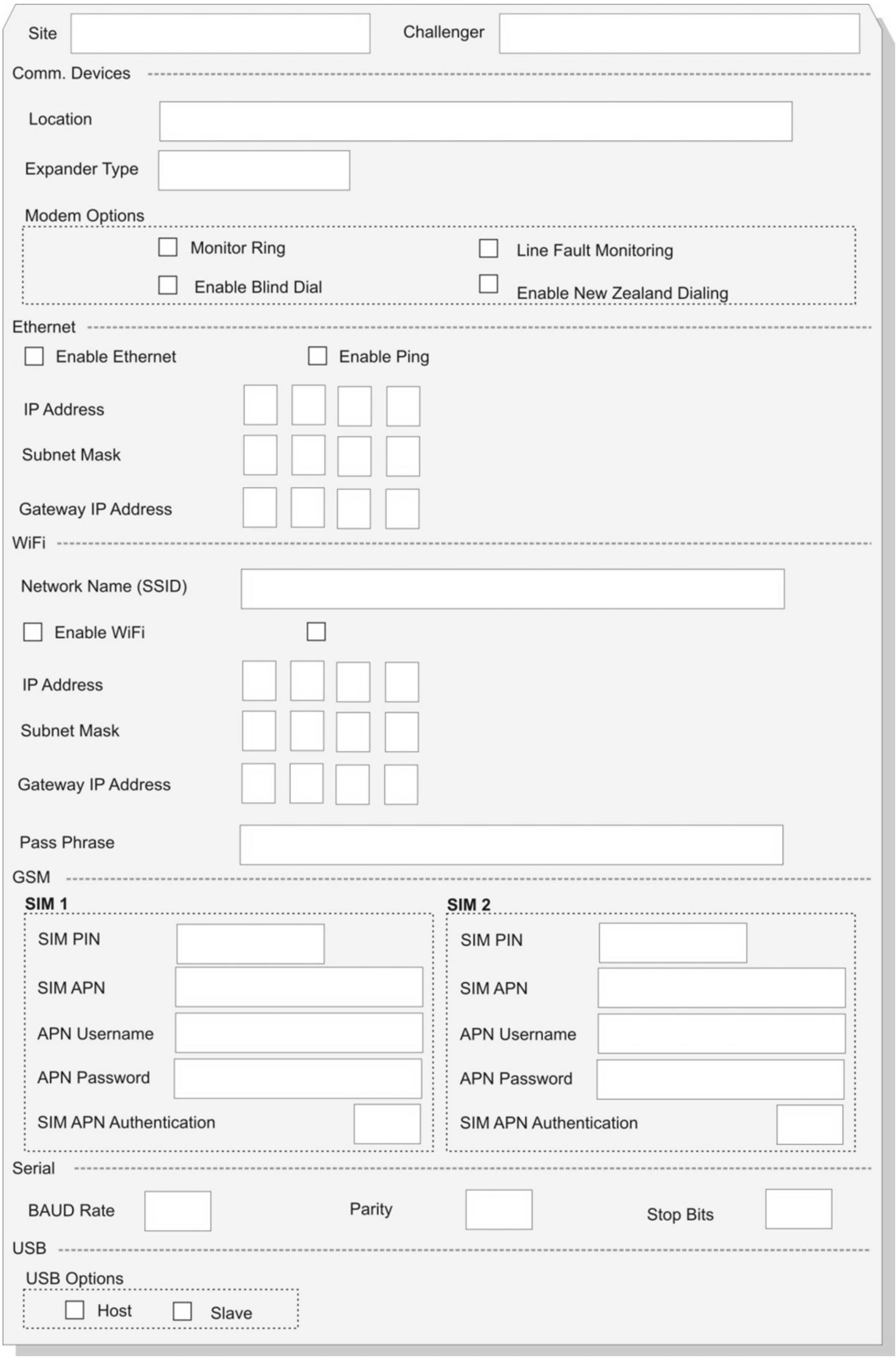
Alarm group name

Auto reset time (m)

Communications worksheets

For programming details see “Option 9: Communications” on page 122.

Figure 39: Communications devices worksheet



Site Challenger

Comm. Devices

Location

Expander Type

Modem Options

□ Monitor Ring □ Line Fault Monitoring

□ Enable Blind Dial □ Enable New Zealand Dialing

Ethernet

□ Enable Ethernet □ Enable Ping

IP Address

Subnet Mask

Gateway IP Address

WiFi

Network Name (SSID)

□ Enable WiFi □

IP Address

Subnet Mask

Gateway IP Address

Pass Phrase

GSM

SIM 1

SIM PIN

SIM APN

APN Username

APN Password

SIM APN Authentication

SIM 2

SIM PIN

SIM APN

APN Username

APN Password

SIM APN Authentication

Serial

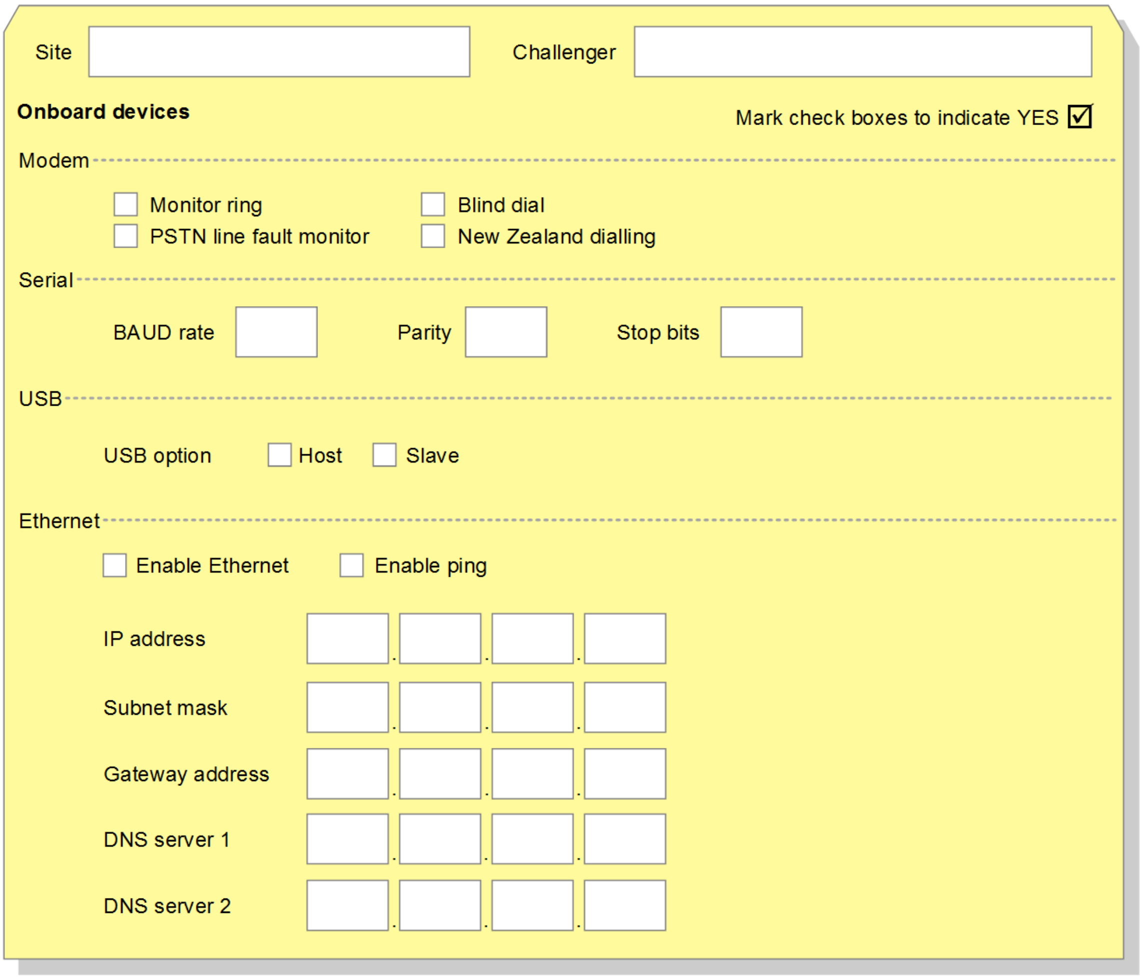
BAUD Rate Parity Stop Bits

USB

USB Options

□ Host □ Slave

Figure 40: Communications devices worksheet (onboard hardware)



Site Challenger

Onboard devices

Mark check boxes to indicate YES ☑

Modem

□ Monitor ring □ Blind dial

□ PSTN line fault monitor □ New Zealand dialling

Serial

BAUD rate Parity Stop bits

USB

USB option □ Host □ Slave

Ethernet

□ Enable Ethernet □ Enable ping

IP address . . .

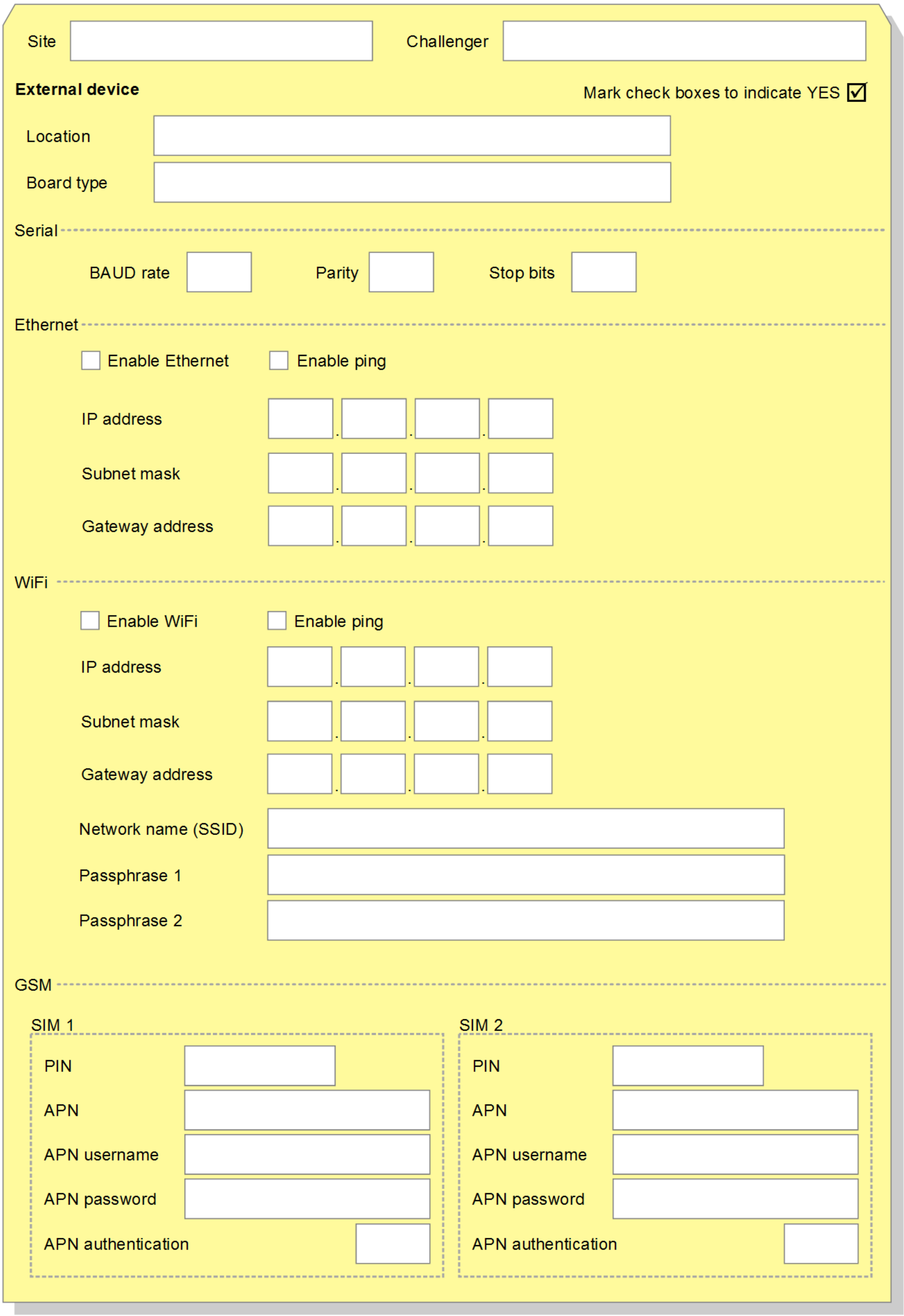
Subnet mask . . .

Gateway address . . .

DNS server 1 . . .

DNS server 2 . . .

Figure 41: Communications devices worksheet (external hardware)



Site ______ Challenger ______

External device

Mark check boxes to indicate YES ☑

Location ______

Board type ______

Serial

BAUD rate ____ Parity ____ Stop bits ____

Ethernet

□ Enable Ethernet □ Enable ping

IP address ____ . ____ . ____ . ____

Subnet mask ____ . ____ . ____ . ____

Gateway address ____ . ____ . ____ . ____

WiFi

□ Enable WiFi □ Enable ping

IP address ____ . ____ . ____ . ____

Subnet mask ____ . ____ . ____ . ____

Gateway address ____ . ____ . ____ . ____

Network name (SSID) ______

Passphrase 1 ______

Passphrase 2 ______

GSM

SIM 1

PIN ______

APN ______

APN username ______

APN password ______

APN authentication ____

SIM 2

PIN ______

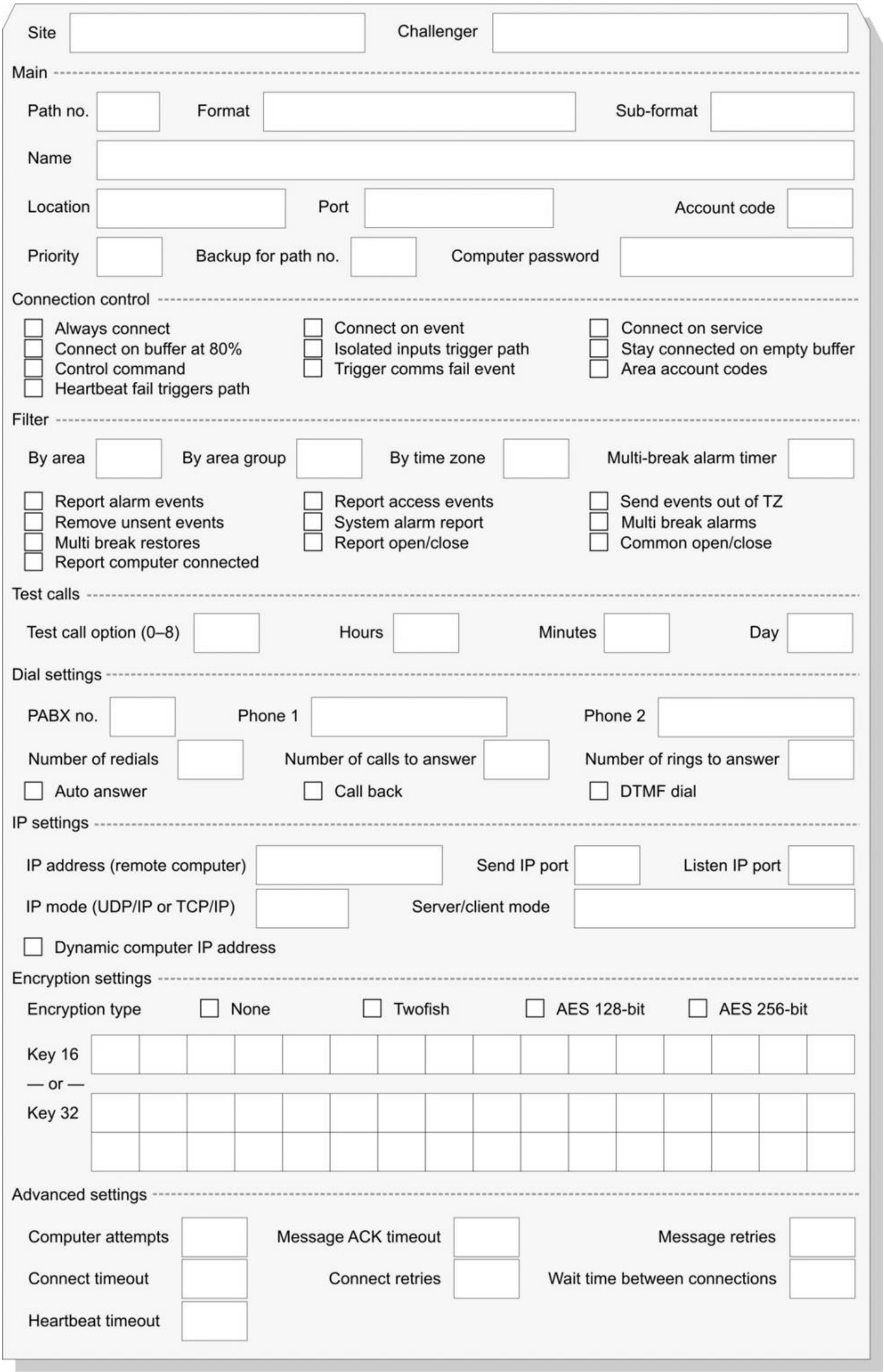
APN ______

APN username ______

APN password ______

APN authentication ____

Figure 42: Communications paths worksheet



Site ______ Challenger ______

Main

Path no. ______ Format ______ Sub-format ______

Name ______

Location ______ Port ______ Account code ______

Priority ______ Backup for path no. ______ Computer password ______

Connection control

□ Always connect
□ Connect on buffer at 80%
□ Control command
□ Heartbeat fail triggers path
□ Connect on event
□ Isolated inputs trigger path
□ Trigger comms fail event
□ Connect on service
□ Stay connected on empty buffer
□ Area account codes

Filter

By area ______ By area group ______ By time zone ______ Multi-break alarm timer ______

□ Report alarm events
□ Remove unsent events
□ Multi break restores
□ Report computer connected
□ Report access events
□ System alarm report
□ Report open/close
□ Send events out of TZ
□ Multi break alarms
□ Common open/close

Test calls

Test call option (0–8) ______ Hours ______ Minutes ______ Day ______

Dial settings

PABX no. ______ Phone 1 ______ Phone 2 ______

Number of redials ______ Number of calls to answer ______ Number of rings to answer ______

□ Auto answer □ Call back □ DTMF dial

IP settings

IP address (remote computer) ______ Send IP port ______ Listen IP port ______

IP mode (UDP/IP or TCP/IP) ______ Server/client mode ______

□ Dynamic computer IP address

Encryption settings

Encryption type □ None □ Twofish □ AES 128-bit □ AES 256-bit

Key 16

— or —

Key 32

Advanced settings

Computer attempts ______ Message ACK timeout ______ Message retries ______

Connect timeout ______ Connect retries ______ Wait time between connections ______

Heartbeat timeout ______

Site　　Challenger

Main

Path number　　Path name　　□ Enabled

Format　　Sub format

Interface location　　Interface port　　Account code

Priority　　Backup for path no.　　Computer password

Connection control

□ Always connect
□ Connect on buffer at 80%
□ Control command
□ Communication event triggers path
□ Connect on event
□ Isolated inputs trigger path
□ Trigger comms fail event flag
□ Connect on service
□ Stay connected on empty buffer
□ Use area account code

Filter

By area　　Or area group　　Event time zone　　Multi break time

□ Report alarm events
□ Remove unsent events
□ Multi break restores
□ Report connection events
□ Report access events
□ Report system alarms
□ Report open/close
□ Report communication events
□ Send events out of TZ
□ Multi break alarms
□ Common open/close
□ Disarm clears pending alarms

Test calls

Test call option (0–8)　　Hours　　Minutes　　Day

Dial settings

PABX no.　　Phone 1　　Phone 2

Number of redials　　Number of calls　　Number of rings

□ Auto answer　□ Call back　□ DTMF dial

IP settings

Send to IP address . . .　　Send port　　Listen port

IP Mode　□ TCP/IP □ UDP/IP　　Server/client mode　□ Server □ Client　　□ Dynamic computer address

Encryption settings

Encryption type　□ None □ Twofish □ AES 128-bit □ AES 256-bit

Key 16

— or —

Key 32

Advanced settings

Computer attempts　　Message ACK timeout (ms)　　Message retries

Connect timeout (s)　　Wait time between connections (s)　　Heartbeat timeout (s)

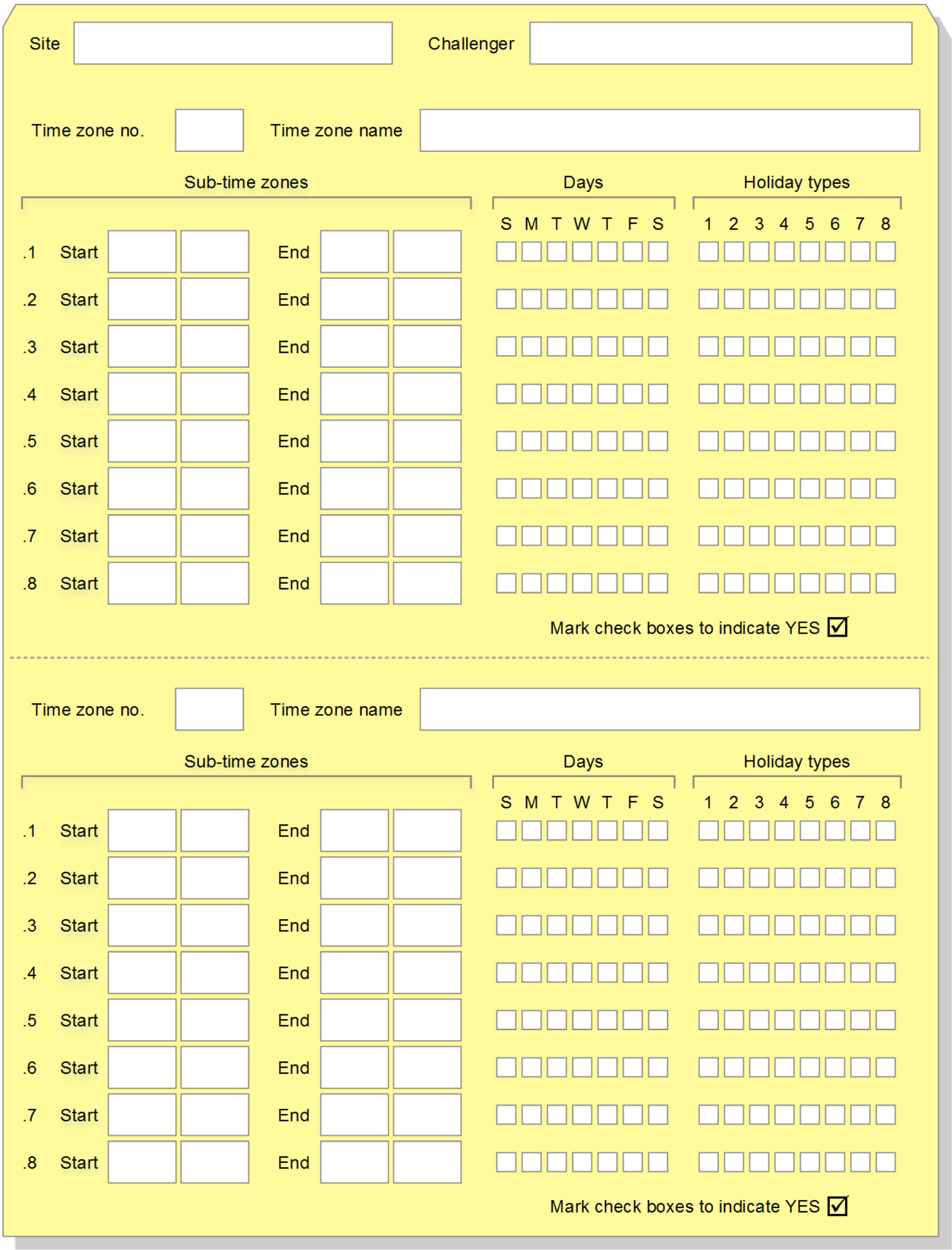
Authentication

Name　　Password

Time zones worksheet

For programming details see “Option 13: Time zones” on page 161.

Figure 43: Time zones worksheet



Site ________ Challenger ________

Time zone no. ____ Time zone name ________

							Days	Holiday types
Sub-time zones							S M T W T F S	1 2 3 4 5 6 7 8
.1	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.2	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.3	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.4	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.5	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.6	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.7	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.8	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □

Mark check boxes to indicate YES ☑

Time zone no. ____ Time zone name ________

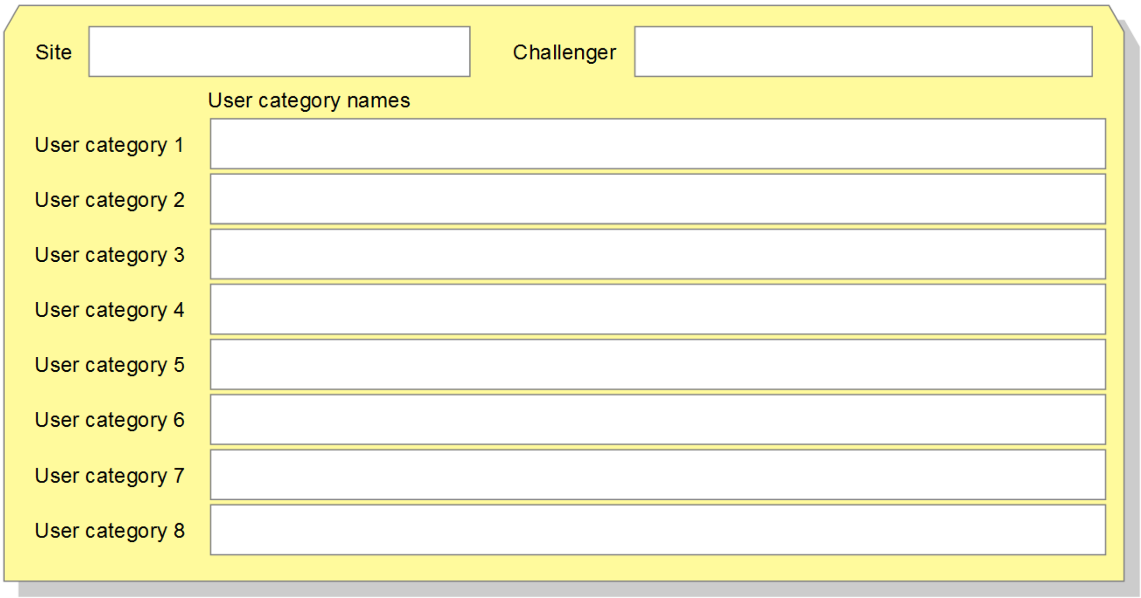
							Days	Holiday types
Sub-time zones							S M T W T F S	1 2 3 4 5 6 7 8
.1	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.2	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.3	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.4	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.5	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.6	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.7	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □
.8	Start			End			□ □ □ □ □ □ □	□ □ □ □ □ □ □ □

Mark check boxes to indicate YES ☑

User categories worksheet

For programming details see “Option 15: User category” on page 163.

Figure 44: User categories worksheet



Site

Challenger

User category names

User category 1

User category 2

User category 3

User category 4

User category 5

User category 6

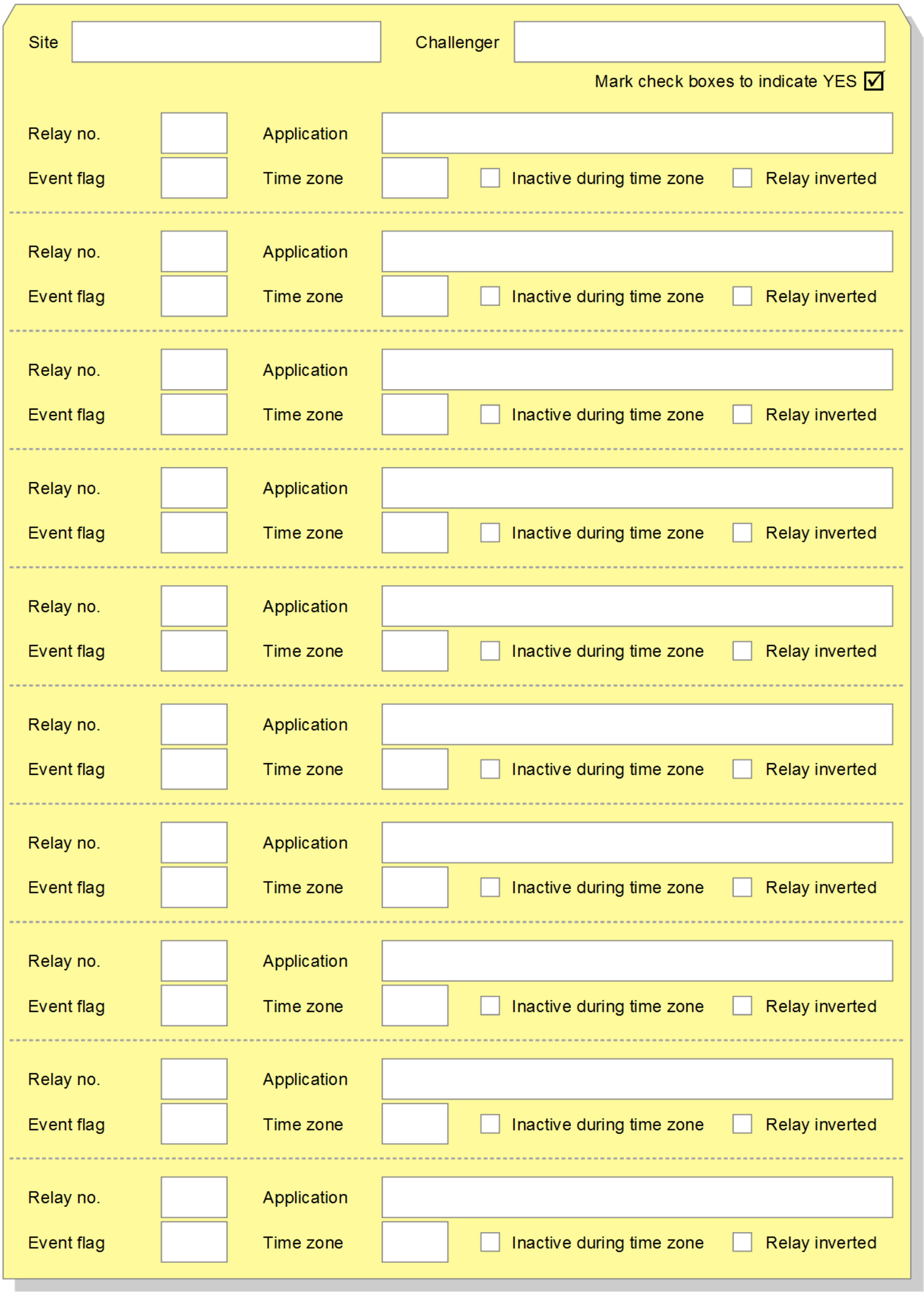
User category 7

User category 8

Relay mapping worksheet

For programming details see “Option 16: Map relays” on page 165.

Figure 45: Relay mapping worksheet



Site Challenger

Mark check boxes to indicate YES ☑

Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

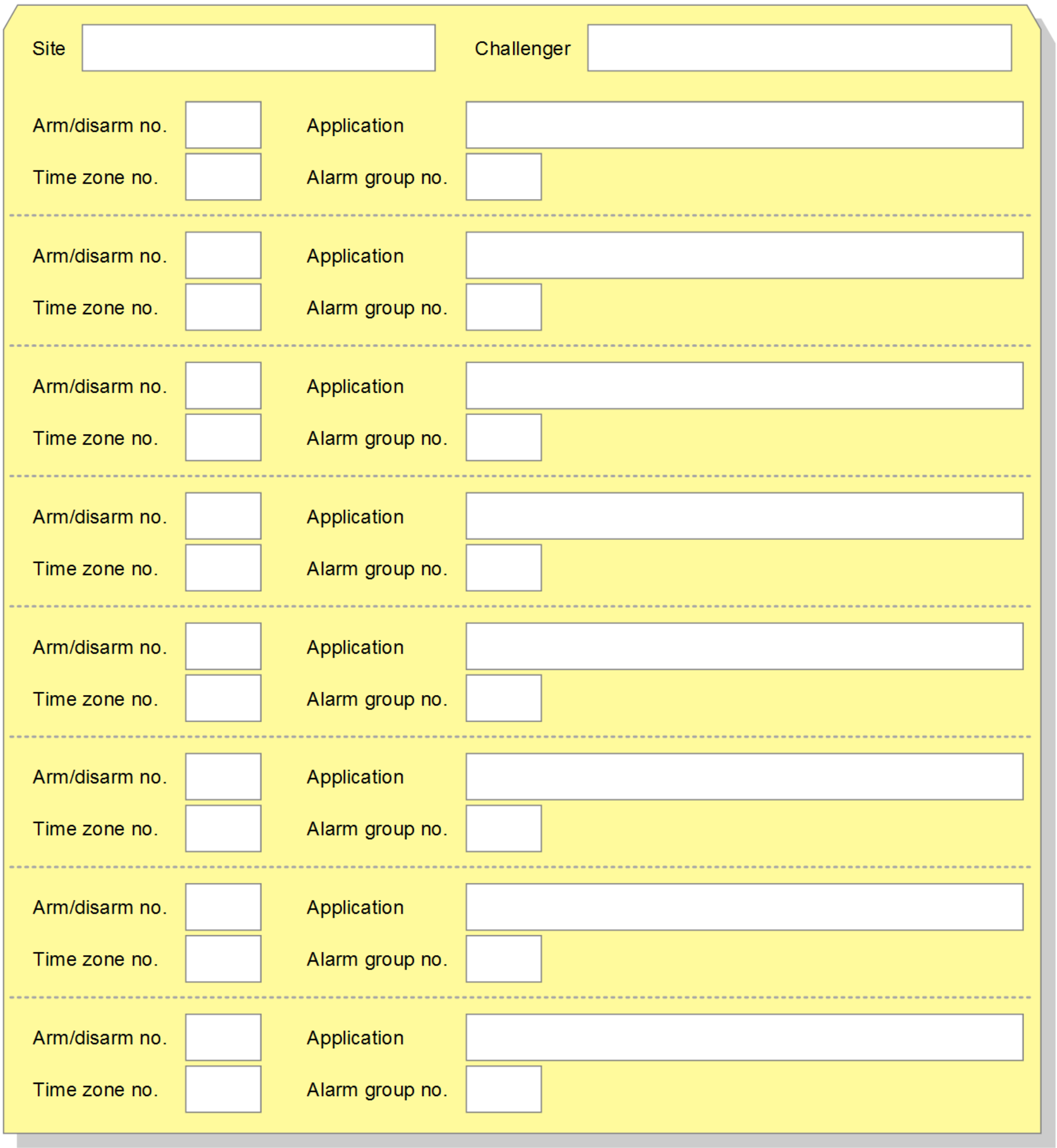
Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

Relay no. Application
Event flag Time zone □ Inactive during time zone □ Relay inverted

Arm or disarm via time zone worksheet

For programming details see “Option 17: Arm/disarm via TZ” on page 167.

Figure 46: Arm or disarm via time zone worksheet



Site Challenger

Arm/disarm no. Application
Time zone no. Alarm group no.

Arm/disarm no. Application
Time zone no. Alarm group no.

Arm/disarm no. Application
Time zone no. Alarm group no.

Arm/disarm no. Application
Time zone no. Alarm group no.

Arm/disarm no. Application
Time zone no. Alarm group no.

Arm/disarm no. Application
Time zone no. Alarm group no.

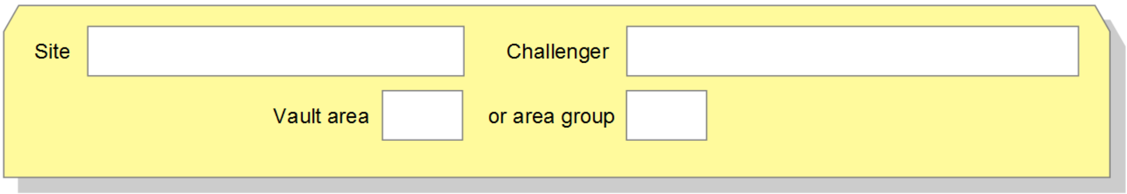
Arm/disarm no. Application
Time zone no. Alarm group no.

Arm/disarm no. Application
Time zone no. Alarm group no.

Vaults worksheet

For programming details see “Option 18: Vaults” on page 169.

Figure 47: Vaults programming worksheet

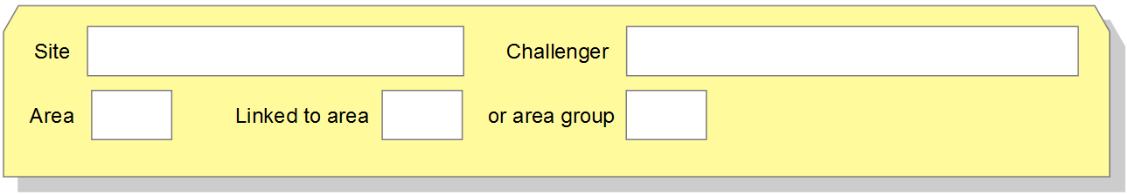


Site		Challenger	
Vault area		or area group	

Area linking worksheet

For programming details see “Option 19: Area linking” on page 170.

Figure 48: Area linking worksheet

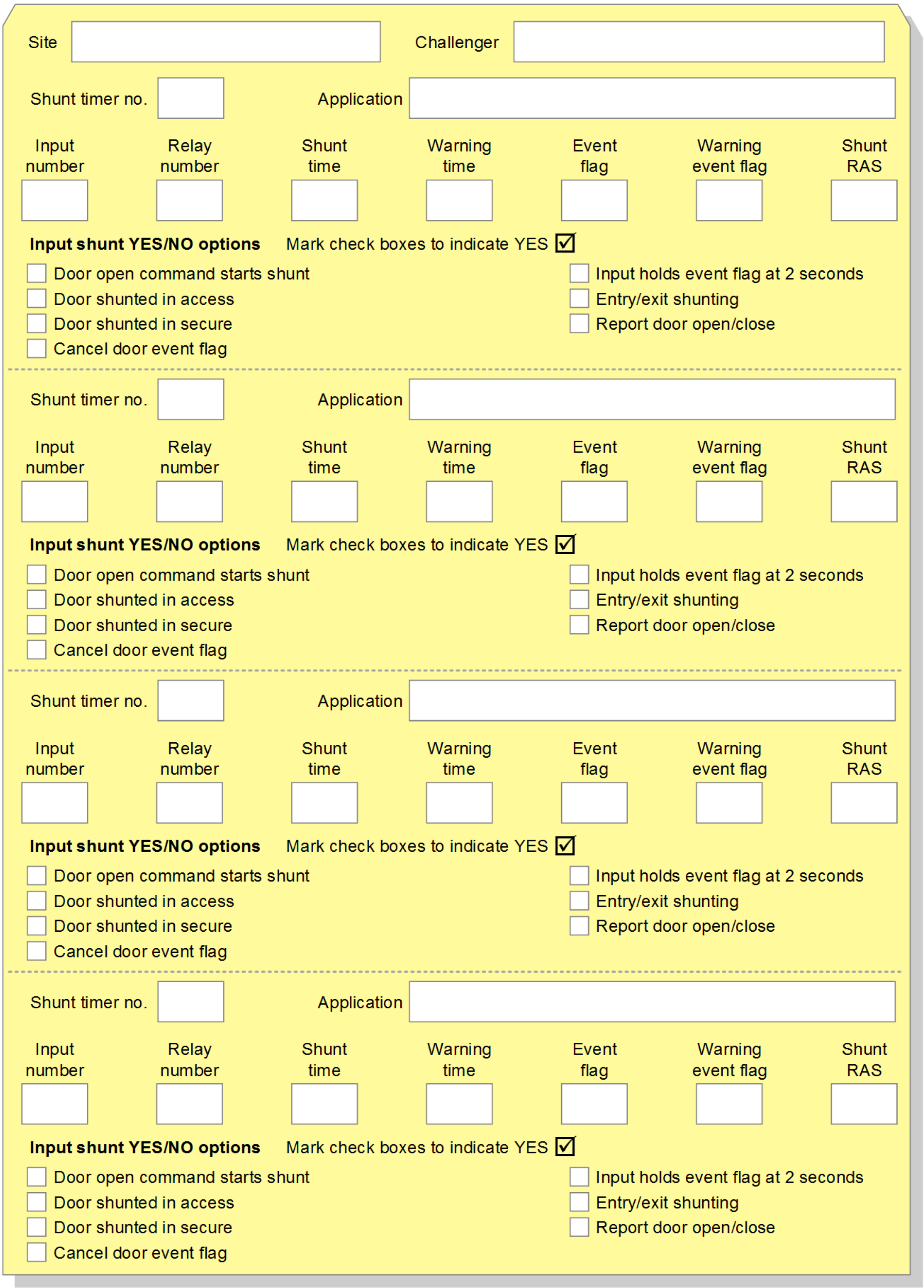


Site			Challenger		
Area		Linked to area		or area group	

Input shunt worksheet

For programming details see "Option 21: Input shunts" on page 171.

Figure 49: Input shunt worksheet



Site

Challenger

Shunt timer no.

Application

Input number	Relay number	Shunt time	Warning time	Event flag	Warning event flag	Shunt RAS

Input shunt YES/NO options Mark check boxes to indicate YES ☑

□ Door open command starts shunt
□ Door shunted in access
□ Door shunted in secure
□ Cancel door event flag
□ Input holds event flag at 2 seconds
□ Entry/exit shunting
□ Report door open/close

Shunt timer no.

Application

Input number	Relay number	Shunt time	Warning time	Event flag	Warning event flag	Shunt RAS

Input shunt YES/NO options Mark check boxes to indicate YES ☑

□ Door open command starts shunt
□ Door shunted in access
□ Door shunted in secure
□ Cancel door event flag
□ Input holds event flag at 2 seconds
□ Entry/exit shunting
□ Report door open/close

Shunt timer no.

Application

Input number	Relay number	Shunt time	Warning time	Event flag	Warning event flag	Shunt RAS

Input shunt YES/NO options Mark check boxes to indicate YES ☑

□ Door open command starts shunt
□ Door shunted in access
□ Door shunted in secure
□ Cancel door event flag
□ Input holds event flag at 2 seconds
□ Entry/exit shunting
□ Report door open/close

Shunt timer no.

Application

Input number	Relay number	Shunt time	Warning time	Event flag	Warning event flag	Shunt RAS

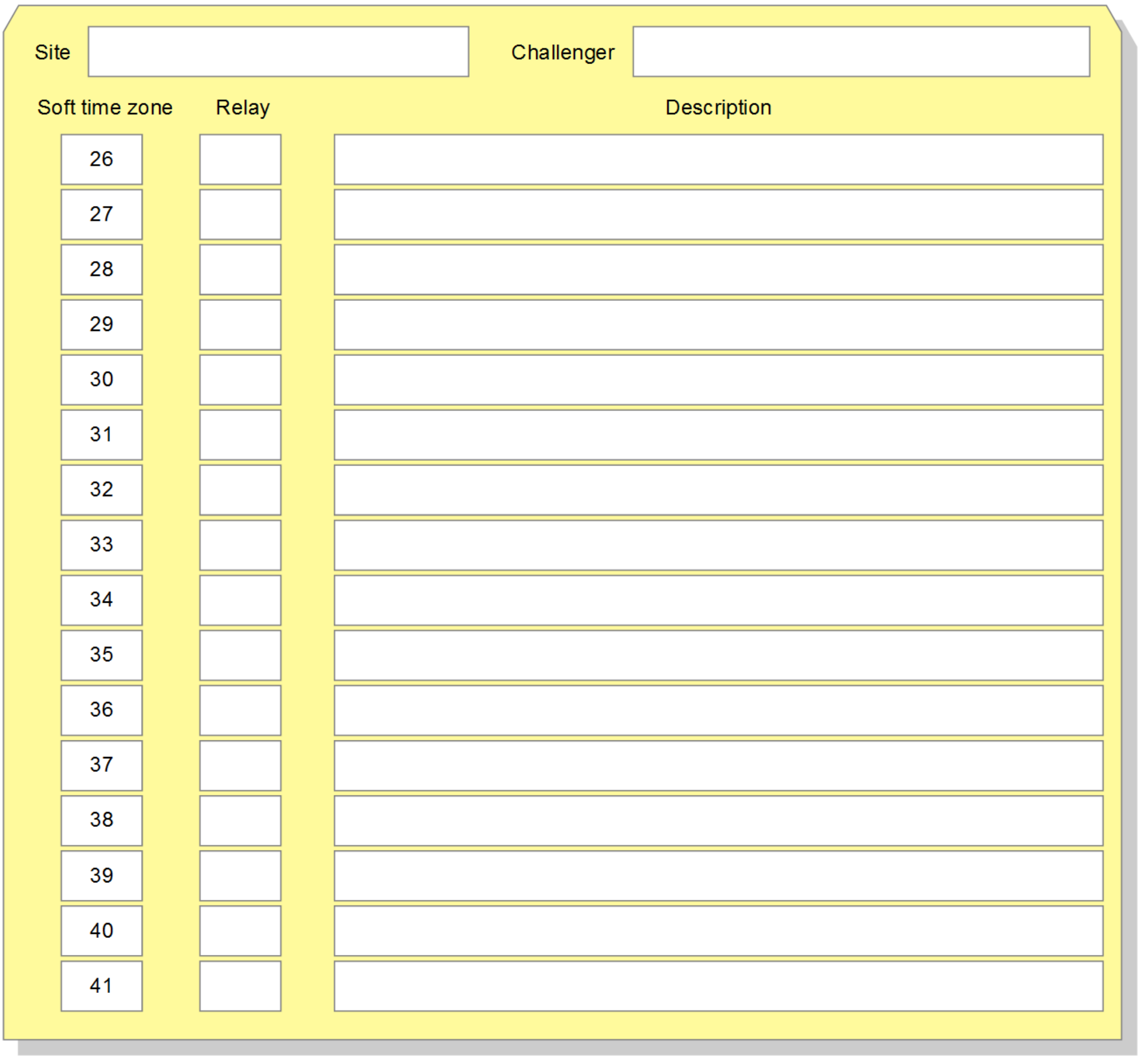
Input shunt YES/NO options Mark check boxes to indicate YES ☑

□ Door open command starts shunt
□ Door shunted in access
□ Door shunted in secure
□ Cancel door event flag
□ Input holds event flag at 2 seconds
□ Entry/exit shunting
□ Report door open/close

Soft time zones worksheet

For programming details see “Option 22: Soft time zones” on page 175.

Figure 50: Time zone to follow relay worksheet



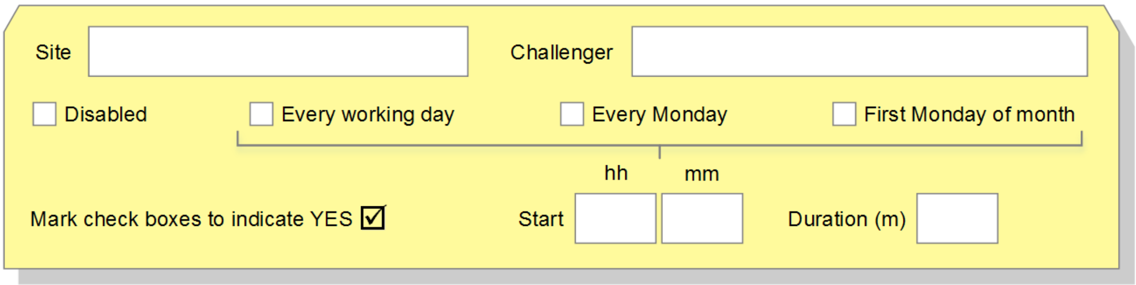
Site ______ Challenger ______

Soft time zone	Relay	Description
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		
36		
37		
38		
39		
40		
41		

Battery testing worksheet

For programming details see “Option 31: Battery testing” on page 179.

Figure 51: Battery testing worksheet



Site ______ Challenger ______

□ Disabled □ Every working day □ Every Monday □ First Monday of month

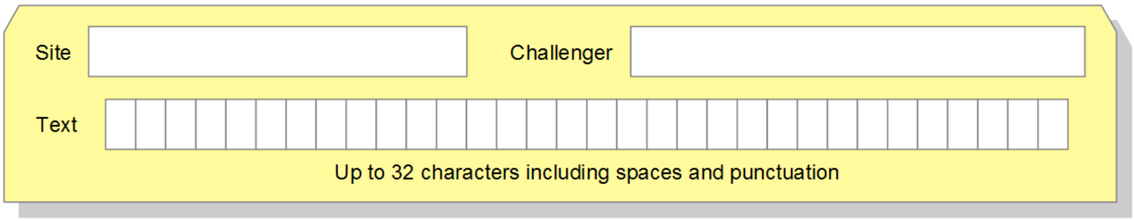
Mark check boxes to indicate YES ☑

Start hh ____ mm ____ Duration (m) ____

Custom message worksheet

For programming details see “Option 32: Custom message” on page 182.

Figure 52: Custom message worksheet



Site

Challenger

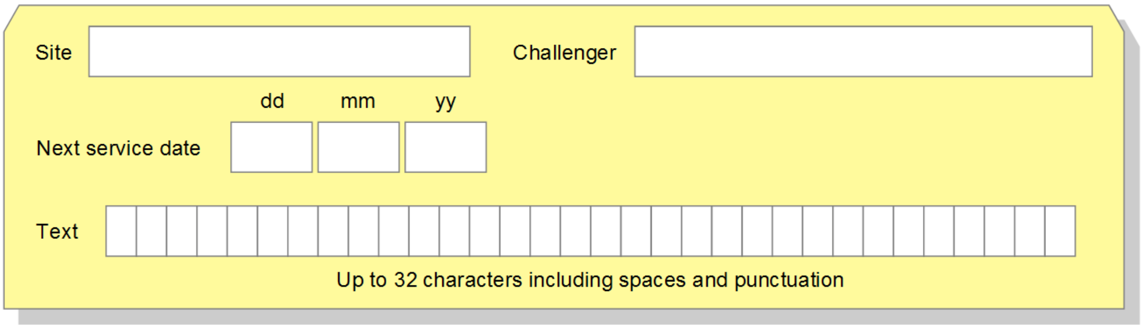
Text

Up to 32 characters including spaces and punctuation

Next service date worksheet

For programming details see “Option 33: Program next service” on page 182.

Figure 53: Next service date worksheet



Site

Challenger

dd mm yy

Next service date

Text

Up to 32 characters including spaces and punctuation

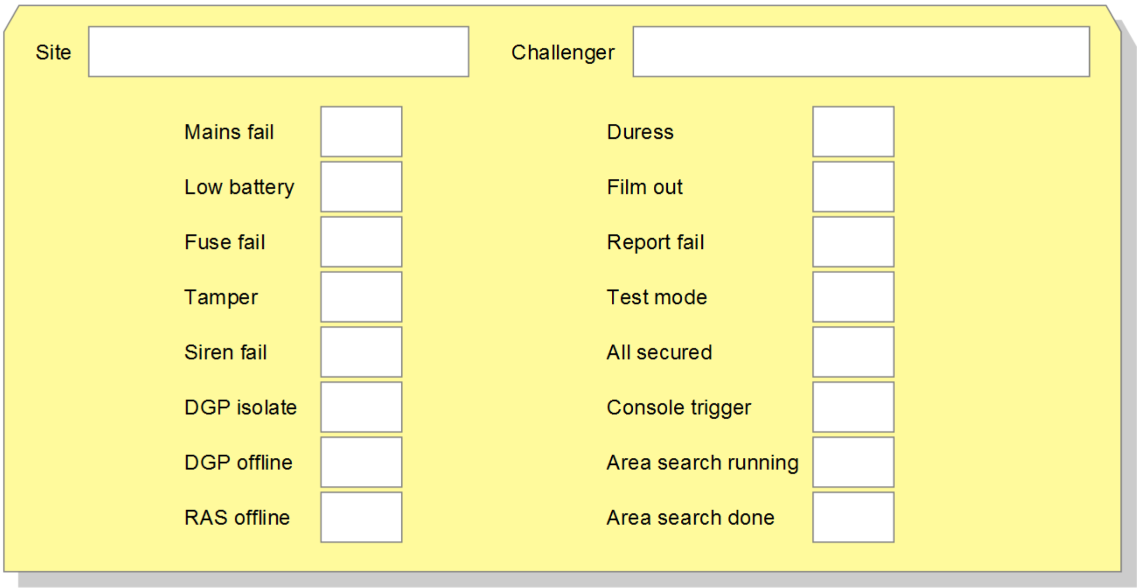
Event flags worksheets

Event flags 1 to 16 have pre-defined functionality as shown in Table 30 on page 243. The functionality is indicated when programming inputs (for example “Event Flag 2, Secure Alarm”). However, they can also be assigned names. Any of the 255 event flags can be assigned names to describe their particular application via “Option 41: Event flag names” on page 200.

Event flags 17 to 255, and some predefined event flags can be used to define either summary (system) events or for outputs to relays or macros.

- Use Figure 54 on page 275 to record the numbers of summary event flags. See “Option 34: Program summary event flags” on page 183 for details.
- Use Figure 55 on page 276 to record the numbers (typically using the same number as the physical relay) and names (or application) of event flags.

Figure 54: Summary event flags worksheet

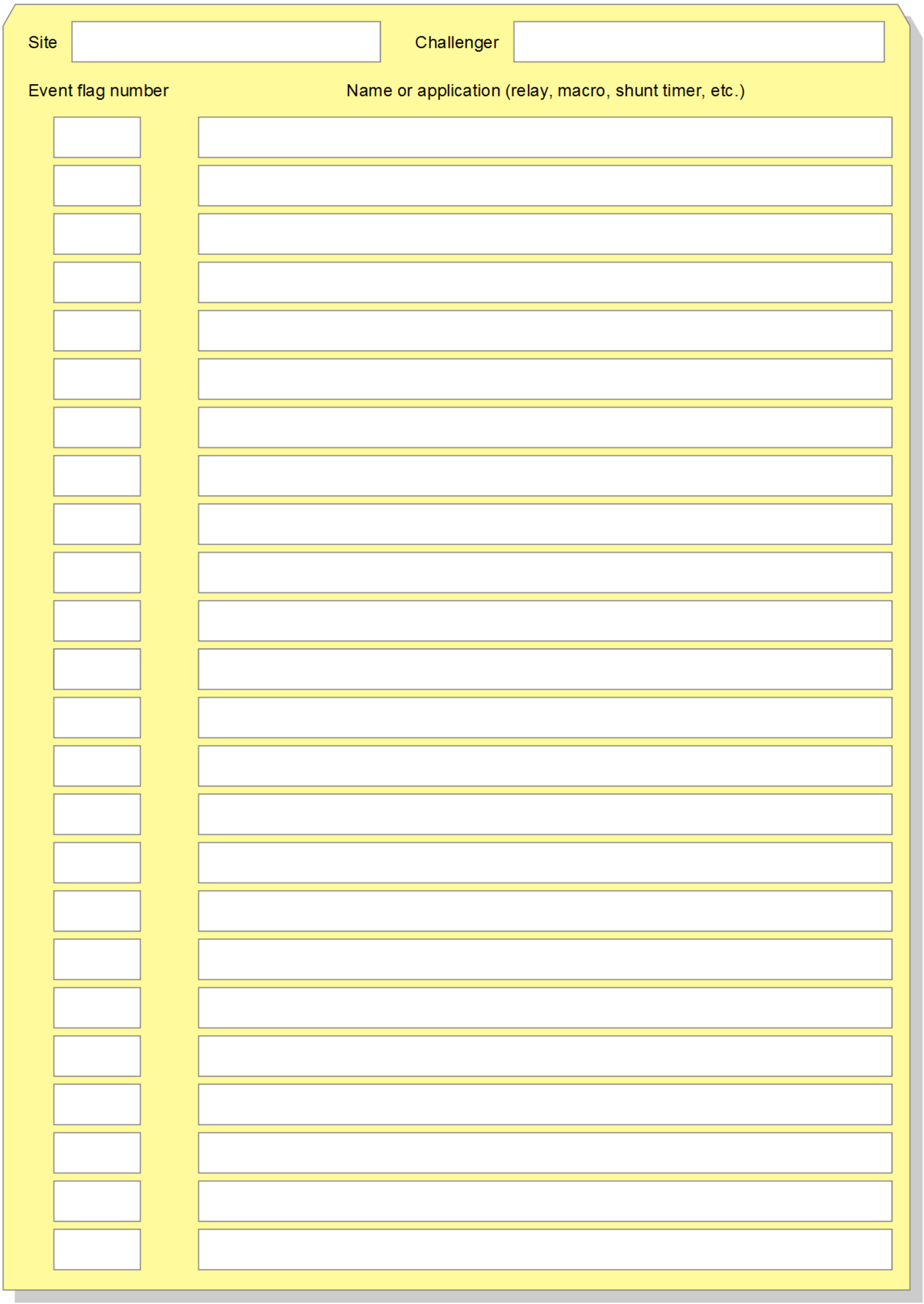


Site

Challenger

Mains fail		Duress	
Low battery		Film out	
Fuse fail		Report fail	
Tamper		Test mode	
Siren fail		All secured	
DGP isolate		Console trigger	
DGP offline		Area search running	
RAS offline		Area search done	

Figure 55: Event flag names worksheet



Site

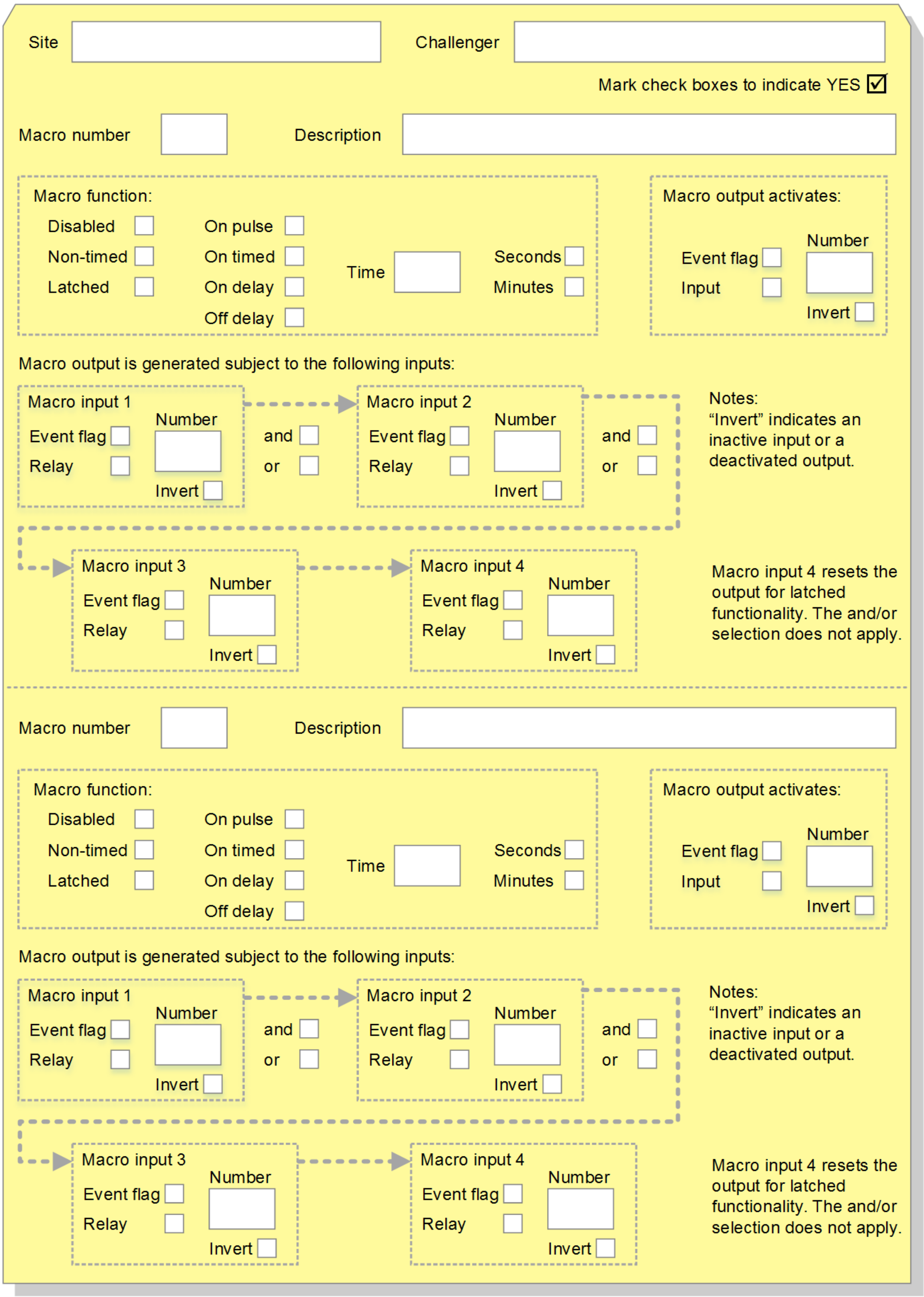
Challenger

Event flag number	Name or application (relay, macro, shunt timer, etc.)

Macro logic worksheet

For programming details see “Option 35: Program macro logic” on page 187.

Figure 56: Macro logic worksheet



Site □ Challenger □

Mark check boxes to indicate YES ☑

Macro number □ Description □

Macro function:

Disabled □ On pulse □

Non-timed □ On timed □ Time □ Seconds □

Latched □ On delay □ Minutes □

Off delay □

Macro output activates:

Event flag □ Number □

Input □

Invert □

Macro output is generated subject to the following inputs:

Macro input 1: Event flag □ Relay □ Number □ Invert □

and □ or □

Macro input 2: Event flag □ Relay □ Number □ Invert □

and □ or □

Notes:
“Invert” indicates an inactive input or a deactivated output.

Macro input 3: Event flag □ Relay □ Number □ Invert □

Macro input 4: Event flag □ Relay □ Number □ Invert □

Macro input 4 resets the output for latched functionality. The and/or selection does not apply.

Macro number □ Description □

Macro function:

Disabled □ On pulse □

Non-timed □ On timed □ Time □ Seconds □

Latched □ On delay □ Minutes □

Off delay □

Macro output activates:

Event flag □ Number □

Input □

Invert □

Macro output is generated subject to the following inputs:

Macro input 1: Event flag □ Relay □ Number □ Invert □

and □ or □

Macro input 2: Event flag □ Relay □ Number □ Invert □

and □ or □

Notes:
“Invert” indicates an inactive input or a deactivated output.

Macro input 3: Event flag □ Relay □ Number □ Invert □

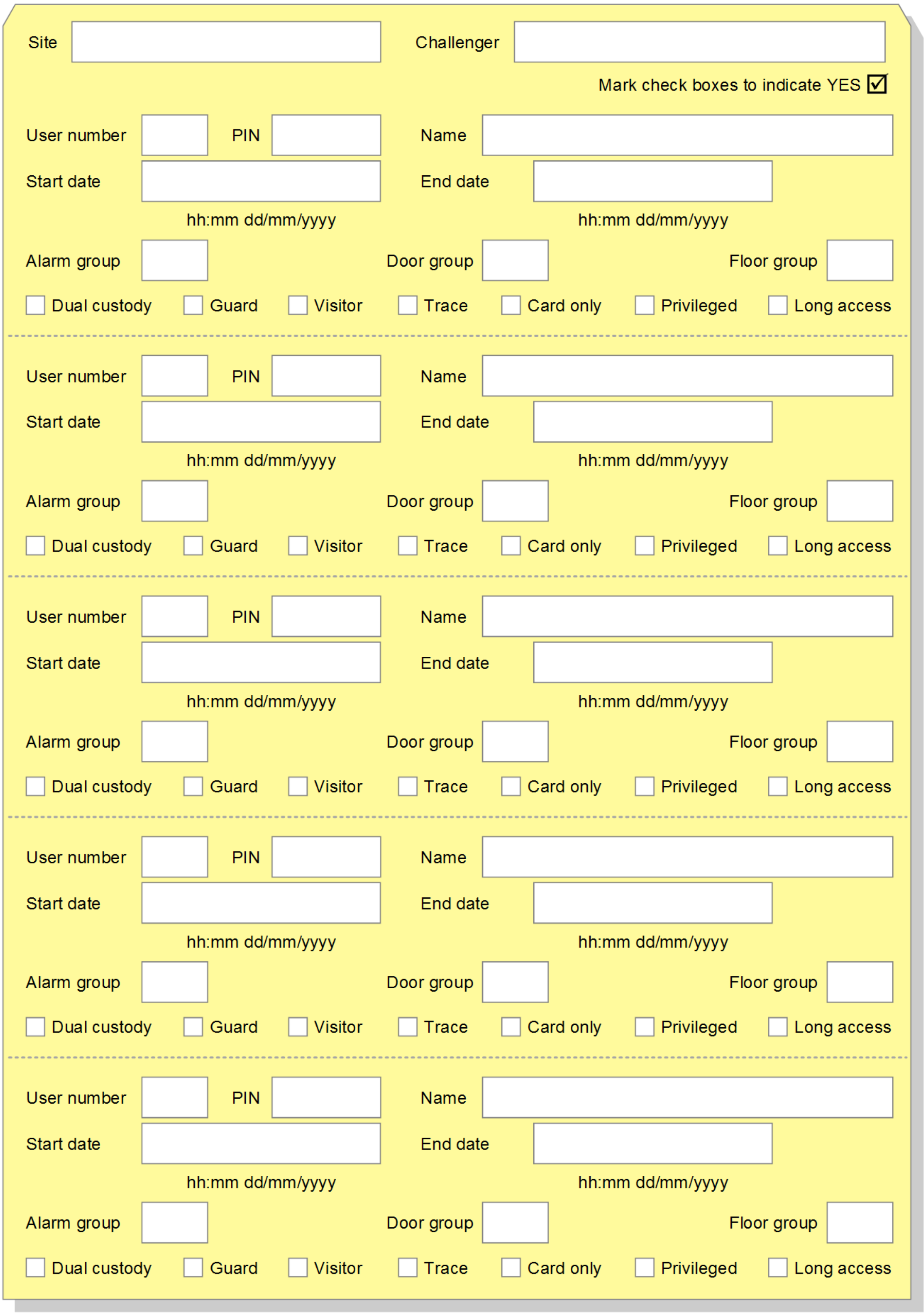
Macro input 4: Event flag □ Relay □ Number □ Invert □

Macro input 4 resets the output for latched functionality. The and/or selection does not apply.

Users worksheet

User records are programmed in user menu option 14. Program Users.

Figure 57: Users worksheet



Site Challenger

Mark check boxes to indicate YES ☑

User number PIN Name

Start date End date

hh:mm dd/mm/yyyy hh:mm dd/mm/yyyy

Alarm group Door group Floor group

□ Dual custody □ Guard □ Visitor □ Trace □ Card only □ Privileged □ Long access

User number PIN Name

Start date End date

hh:mm dd/mm/yyyy hh:mm dd/mm/yyyy

Alarm group Door group Floor group

□ Dual custody □ Guard □ Visitor □ Trace □ Card only □ Privileged □ Long access

User number PIN Name

Start date End date

hh:mm dd/mm/yyyy hh:mm dd/mm/yyyy

Alarm group Door group Floor group

□ Dual custody □ Guard □ Visitor □ Trace □ Card only □ Privileged □ Long access

User number PIN Name

Start date End date

hh:mm dd/mm/yyyy hh:mm dd/mm/yyyy

Alarm group Door group Floor group

□ Dual custody □ Guard □ Visitor □ Trace □ Card only □ Privileged □ Long access

User number PIN Name

Start date End date

hh:mm dd/mm/yyyy hh:mm dd/mm/yyyy

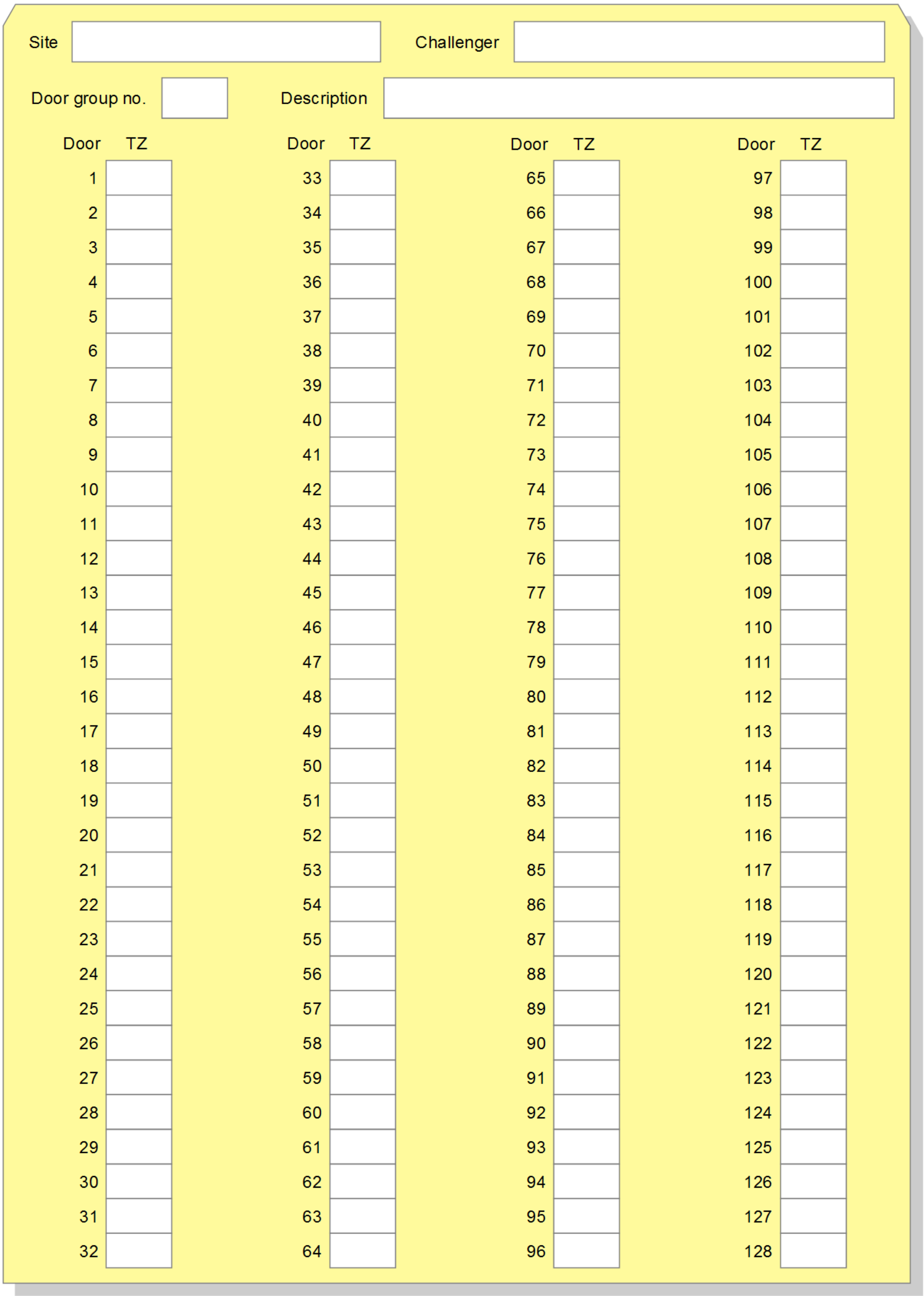
Alarm group Door group Floor group

□ Dual custody □ Guard □ Visitor □ Trace □ Card only □ Privileged □ Long access

Door groups worksheet

Door groups are programmed in user menu option 20. Door and Floor Groups. Challenger panels support 255 door groups.

Figure 58: Door groups 1 to 128 worksheet



Site

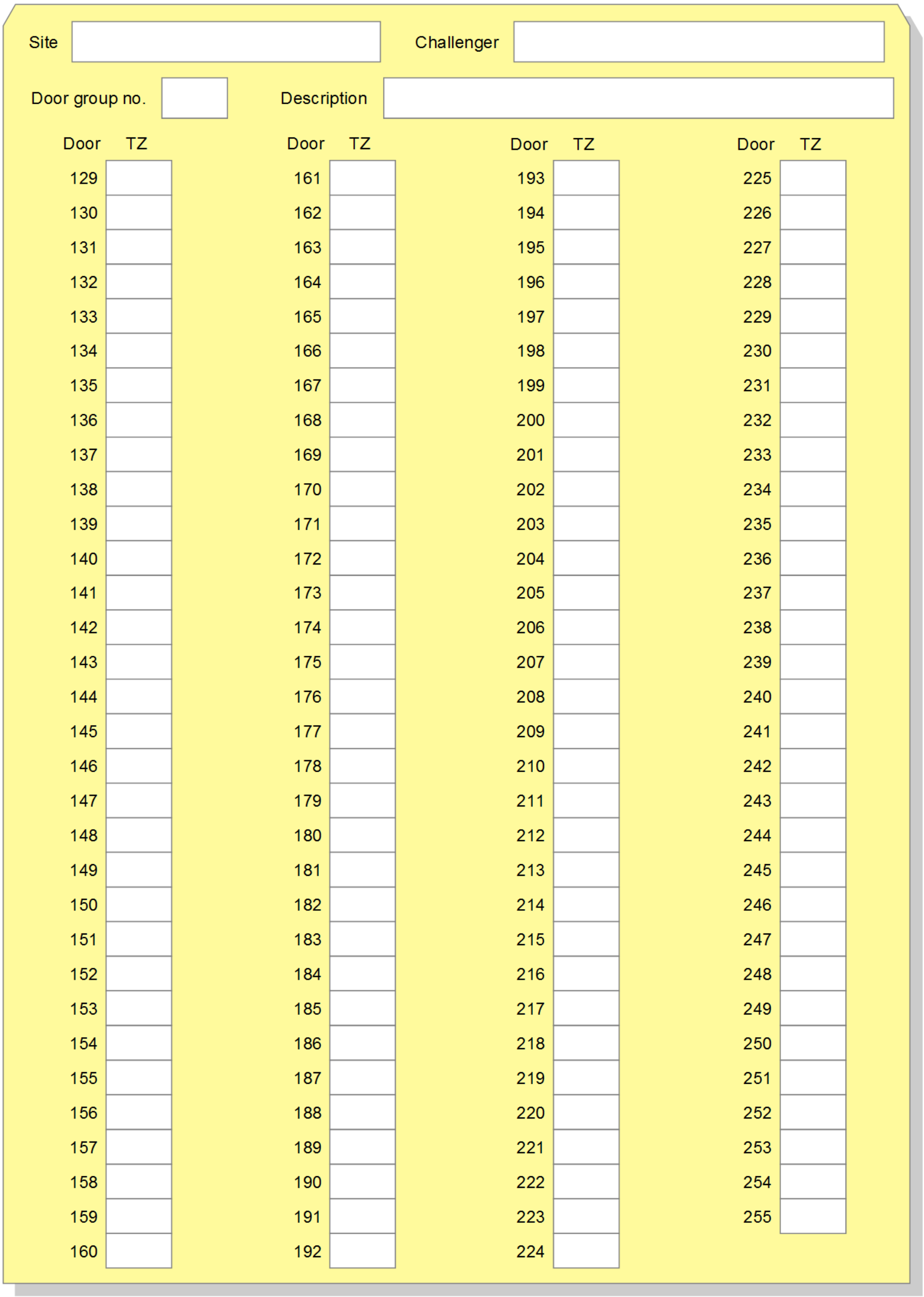
Challenger

Door group no.

Description

Door	TZ	Door	TZ	Door	TZ	Door	TZ
1		33		65		97	
2		34		66		98	
3		35		67		99	
4		36		68		100	
5		37		69		101	
6		38		70		102	
7		39		71		103	
8		40		72		104	
9		41		73		105	
10		42		74		106	
11		43		75		107	
12		44		76		108	
13		45		77		109	
14		46		78		110	
15		47		79		111	
16		48		80		112	
17		49		81		113	
18		50		82		114	
19		51		83		115	
20		52		84		116	
21		53		85		117	
22		54		86		118	
23		55		87		119	
24		56		88		120	
25		57		89		121	
26		58		90		122	
27		59		91		123	
28		60		92		124	
29		61		93		125	
30		62		94		126	
31		63		95		127	
32		64		96		128	

Figure 59: Door groups 129 to 255 worksheet



Site

Challenger

Door group no.

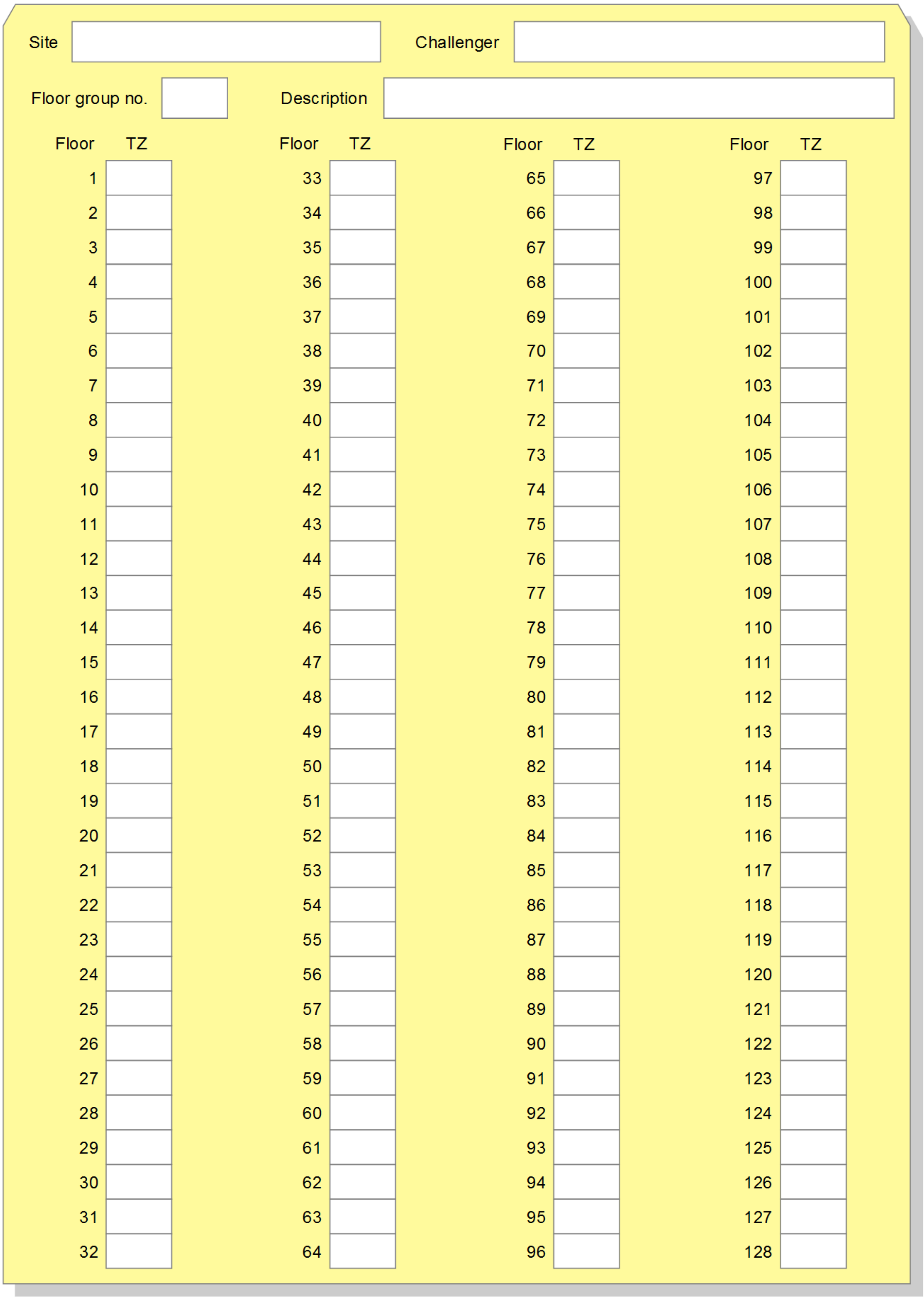
Description

Door	TZ	Door	TZ	Door	TZ	Door	TZ
129		161		193		225	
130		162		194		226	
131		163		195		227	
132		164		196		228	
133		165		197		229	
134		166		198		230	
135		167		199		231	
136		168		200		232	
137		169		201		233	
138		170		202		234	
139		171		203		235	
140		172		204		236	
141		173		205		237	
142		174		206		238	
143		175		207		239	
144		176		208		240	
145		177		209		241	
146		178		210		242	
147		179		211		243	
148		180		212		244	
149		181		213		245	
150		182		214		246	
151		183		215		247	
152		184		216		248	
153		185		217		249	
154		186		218		250	
155		187		219		251	
156		188		220		252	
157		189		221		253	
158		190		222		254	
159		191		223		255	
160		192		224			

Floor groups worksheet

Floor groups are programmed in user menu option 20. Door and Floor Groups. Challenger panels support 128 floor groups.

Figure 60: Floor groups worksheet



Site

Challenger

Floor group no.

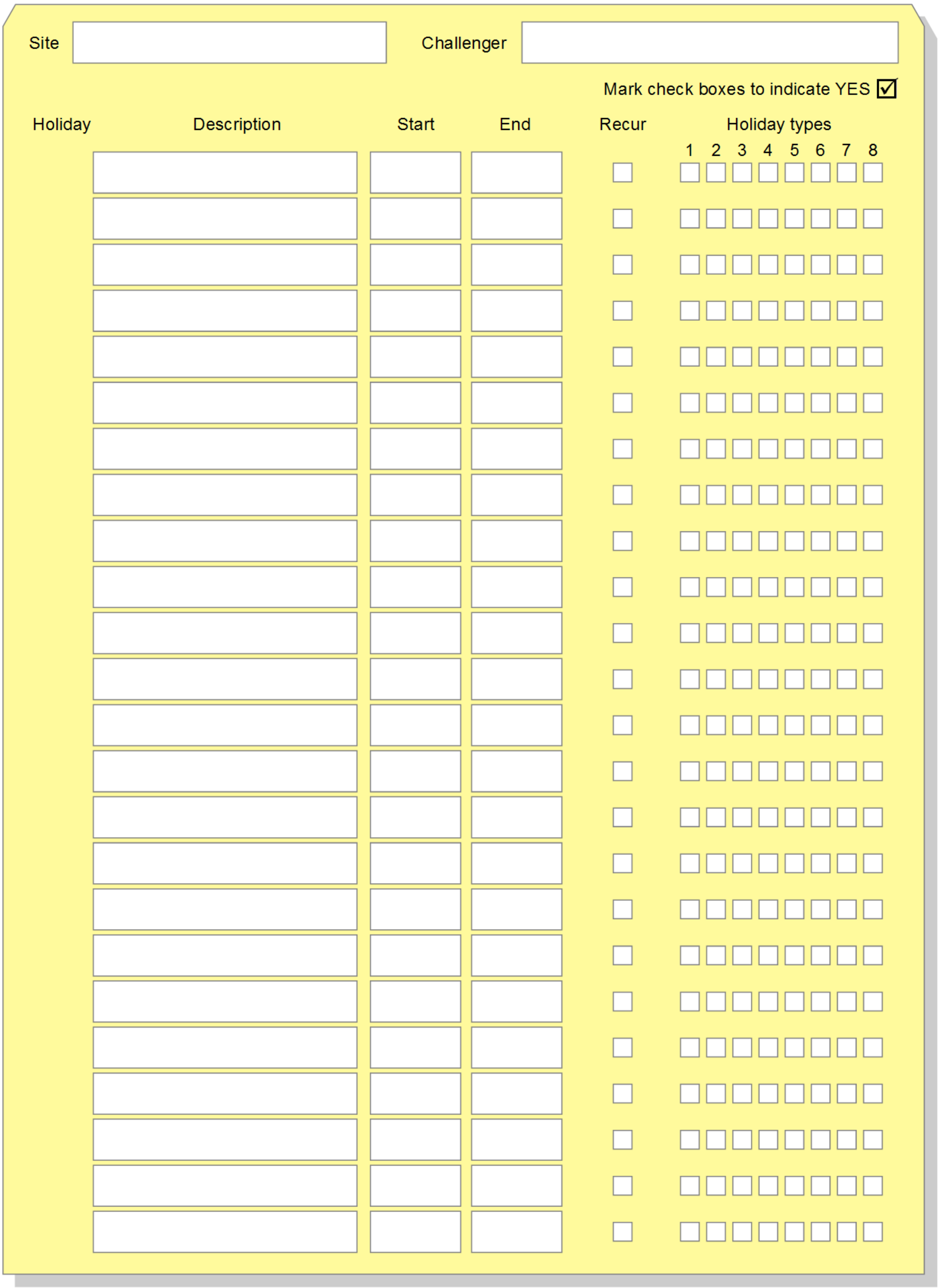
Description

Floor	TZ	Floor	TZ	Floor	TZ	Floor	TZ
1		33		65		97	
2		34		66		98	
3		35		67		99	
4		36		68		100	
5		37		69		101	
6		38		70		102	
7		39		71		103	
8		40		72		104	
9		41		73		105	
10		42		74		106	
11		43		75		107	
12		44		76		108	
13		45		77		109	
14		46		78		110	
15		47		79		111	
16		48		80		112	
17		49		81		113	
18		50		82		114	
19		51		83		115	
20		52		84		116	
21		53		85		117	
22		54		86		118	
23		55		87		119	
24		56		88		120	
25		57		89		121	
26		58		90		122	
27		59		91		123	
28		60		92		124	
29		61		93		125	
30		62		94		126	
31		63		95		127	
32		64		96		128	

Holidays worksheet

Holiday records are programmed in user menu option 21. Holidays.

Figure 61: Holidays worksheet



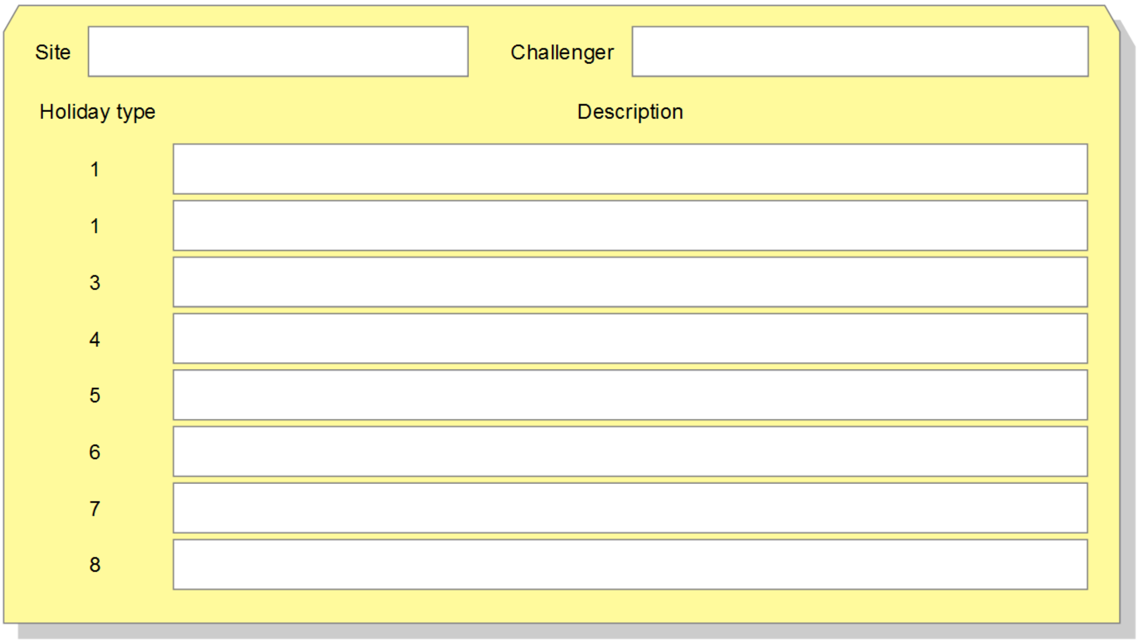
Site

Challenger

Mark check boxes to indicate YES ☑

Holiday	Description	Start	End	Recur	Holiday types							
					1	2	3	4	5	6	7	8
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□
				□	□	□	□	□	□	□	□	□

Figure 62: Holiday types worksheet



Site

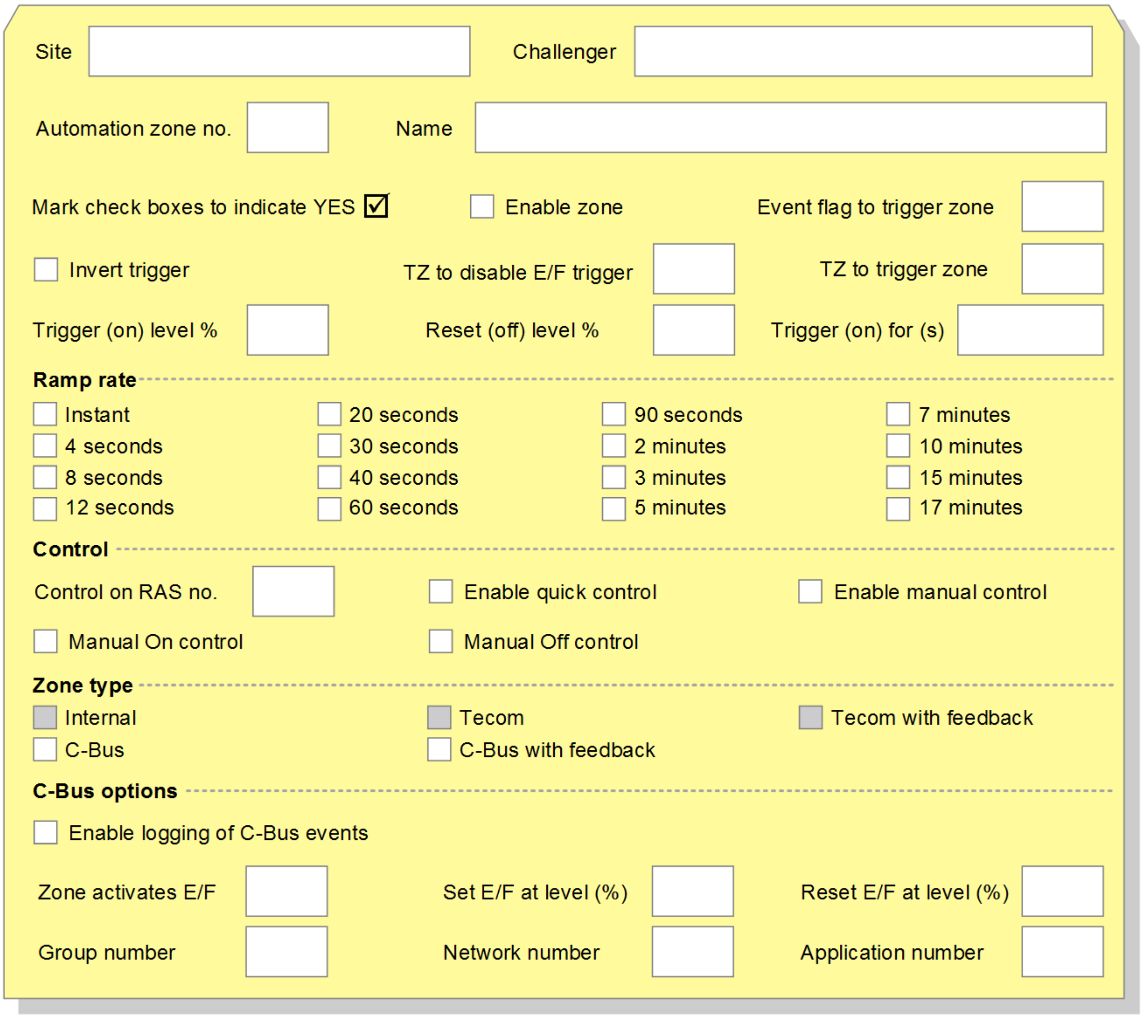
Challenger

Holiday type	Description
1	
1	
3	
4	
5	
6	
7	
8	

Automation zones worksheet

Automation zones are programmed in “Option 39: Automation” on page 193.

Figure 63: Automation zones worksheet



Site

Challenger

Automation zone no.

Name

Mark check boxes to indicate YES ☑

□ Enable zone

Event flag to trigger zone

□ Invert trigger

TZ to disable E/F trigger

TZ to trigger zone

Trigger (on) level %

Reset (off) level %

Trigger (on) for (s)

Ramp rate

□ Instant

□ 4 seconds

□ 8 seconds

□ 12 seconds

□ 20 seconds

□ 30 seconds

□ 40 seconds

□ 60 seconds

□ 90 seconds

□ 2 minutes

□ 3 minutes

□ 5 minutes

□ 7 minutes

□ 10 minutes

□ 15 minutes

□ 17 minutes

Control

Control on RAS no.

□ Enable quick control

□ Enable manual control

□ Manual On control

□ Manual Off control

Zone type

▨ Internal

□ C-Bus

▨ Tecom

□ C-Bus with feedback

▨ Tecom with feedback

C-Bus options

□ Enable logging of C-Bus events

Zone activates E/F

Set E/F at level (%)

Reset E/F at level (%)

Group number

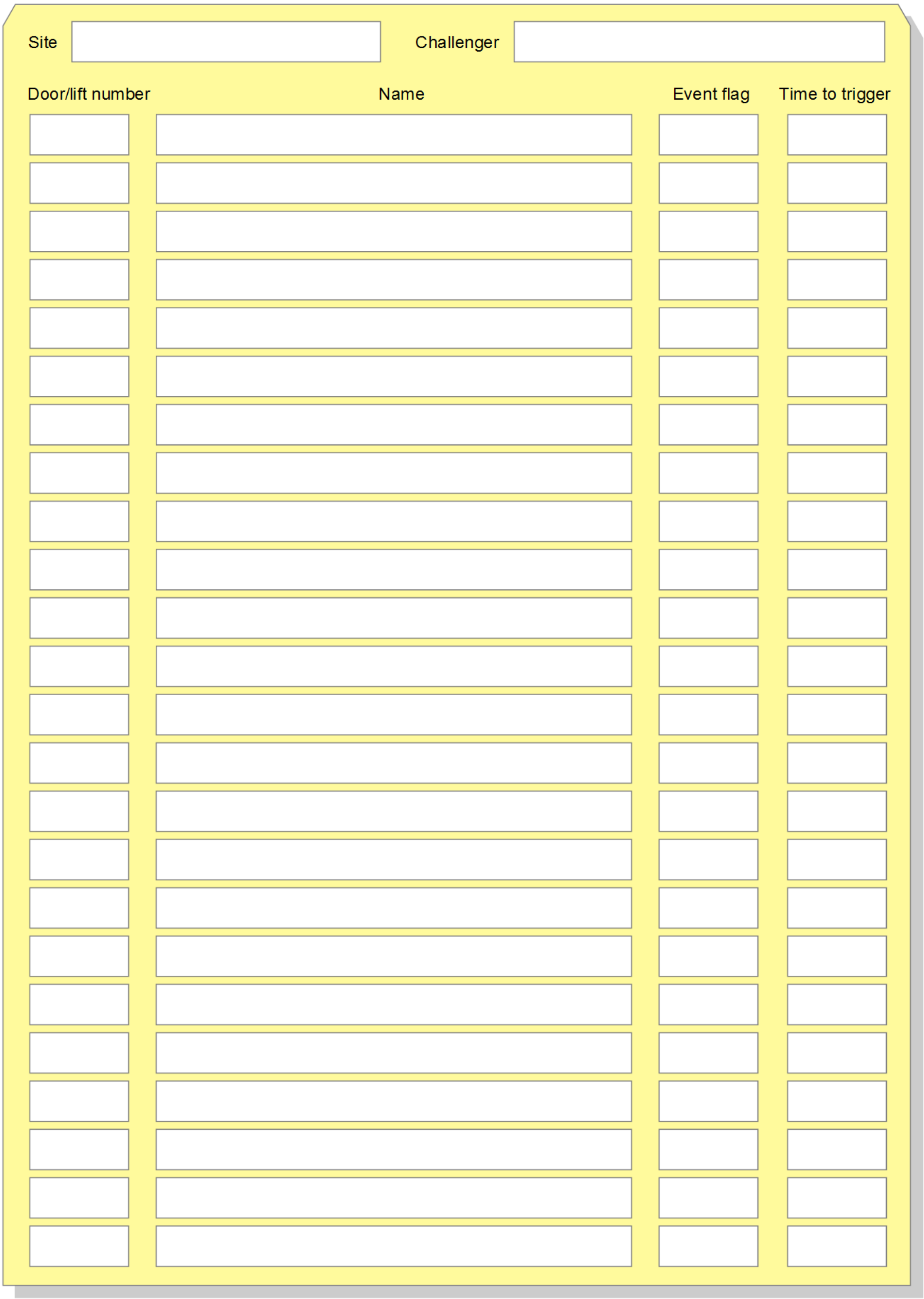
Network number

Application number

Doors & lifts worksheet

Doors are programmed in “Option 40: Door/lift names and E/F trigger” on page 199.

Figure 64: Doors & lifts worksheet



Site

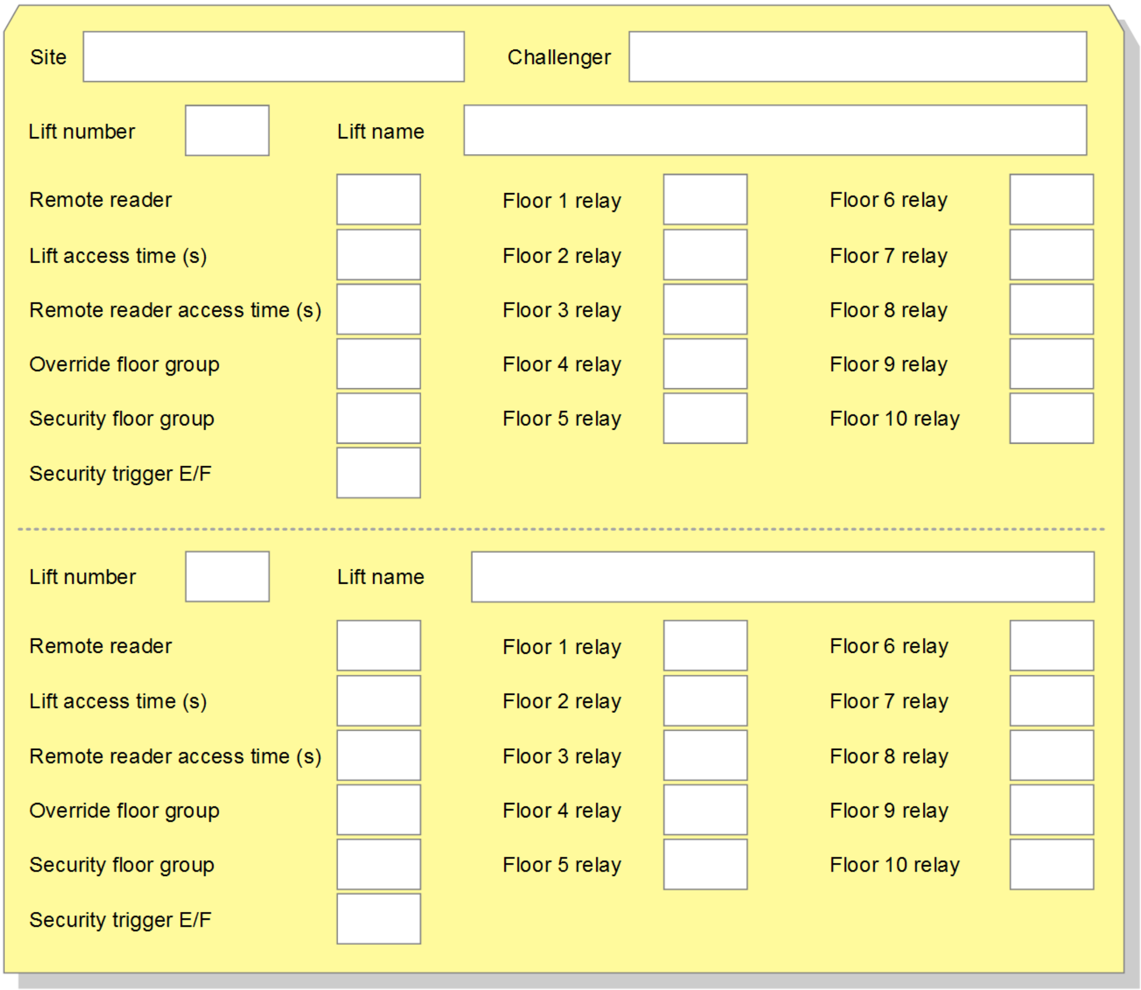
Challenger

Door/lift number	Name	Event flag	Time to trigger

Standard lifts worksheet

Standard lifts are programmed in “Option 44: Standard lifts” on page 201.

Figure 65: Standard lifts worksheet

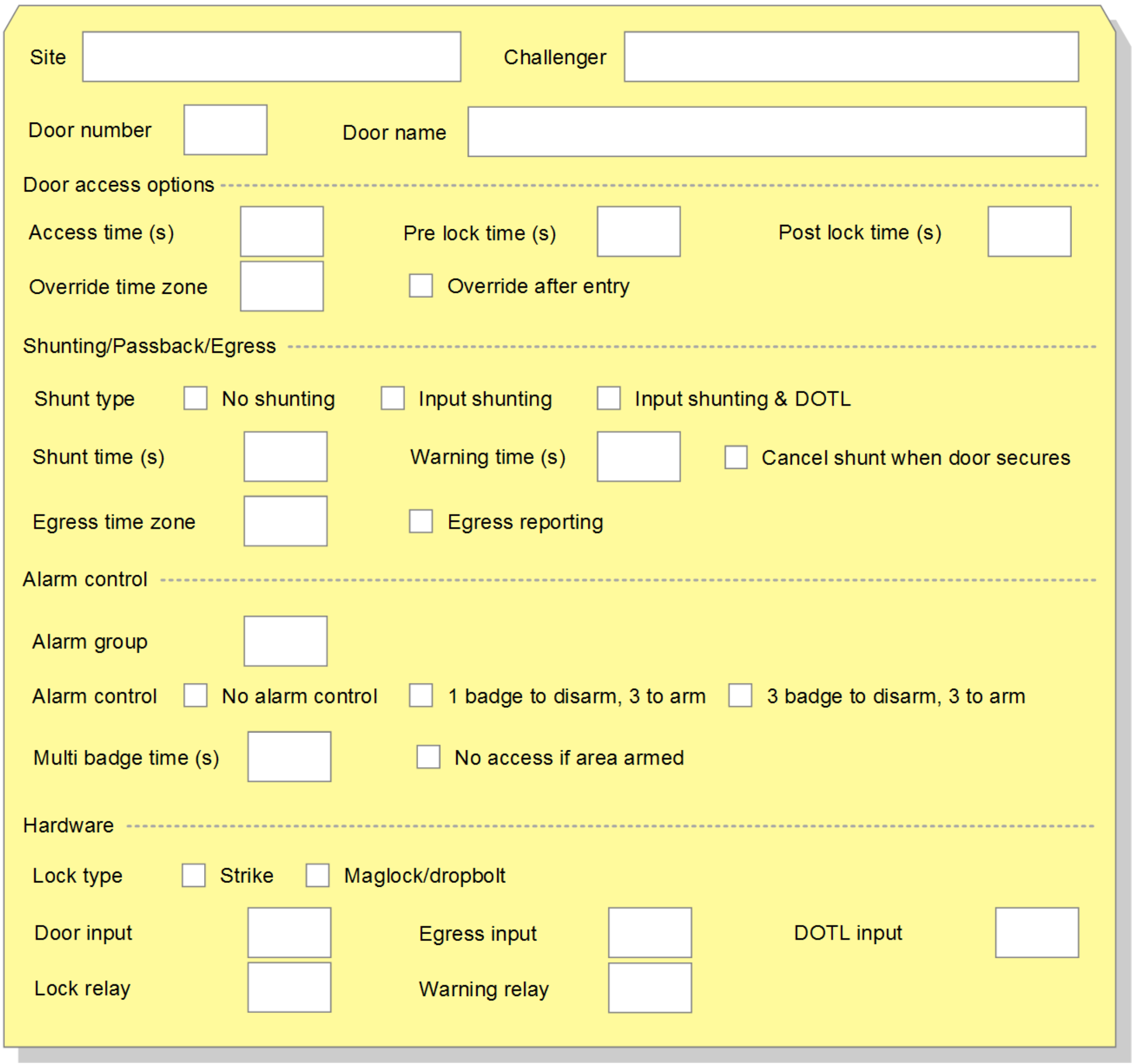


Site		Challenger			
Lift number		Lift name			
Remote reader		Floor 1 relay		Floor 6 relay	
Lift access time (s)		Floor 2 relay		Floor 7 relay	
Remote reader access time (s)		Floor 3 relay		Floor 8 relay	
Override floor group		Floor 4 relay		Floor 9 relay	
Security floor group		Floor 5 relay		Floor 10 relay	
Security trigger E/F					
Lift number		Lift name			
Remote reader		Floor 1 relay		Floor 6 relay	
Lift access time (s)		Floor 2 relay		Floor 7 relay	
Remote reader access time (s)		Floor 3 relay		Floor 8 relay	
Override floor group		Floor 4 relay		Floor 9 relay	
Security floor group		Floor 5 relay		Floor 10 relay	
Security trigger E/F					

Standard doors worksheet

Standard lifts are programmed in “Option 45: Standard doors” on page 204.

Figure 66: Standard doors worksheet



Site

Challenger

Door number

Door name

Door access options

Access time (s)

Pre lock time (s)

Post lock time (s)

Override time zone

□ Override after entry

Shunting/Passback/Egress

Shunt type □ No shunting □ Input shunting □ Input shunting & DOTL

Shunt time (s)

Warning time (s)

□ Cancel shunt when door secures

Egress time zone

□ Egress reporting

Alarm control

Alarm group

Alarm control □ No alarm control □ 1 badge to disarm, 3 to arm □ 3 badge to disarm, 3 to arm

Multi badge time (s)

□ No access if area armed

Hardware

Lock type □ Strike □ Maglock/dropbolt

Door input

Egress input

DOTL input

Lock relay

Warning relay

Glossary

2-state monitoring	The system’s input circuits are monitored for sealed and unsealed conditions.
4-state monitoring	The system’s input circuits are monitored for sealed, unsealed, open, and short conditions. 4-state monitoring (also called input tamper monitoring) is used in Challenger systems by default. See “input tamper”.
24-hour alarm	Input types that will generate an alarm regardless of area status (armed or disarmed).
4-Door/Lift DGP	See “Intelligent Access Controller“.
Access	The state of an area when it’s disarmed. The condition of an area when it is occupied and when the intrusion detection system has been set so that normal activity does not generate an alarm. Opposite of “secure”.
Access control	Control of entry to, or exit from, a security area. The Challenger system typically controls access by allowing only authorised users to unlock a door or to enter a lift.
Access test	The access (disarmed) test is a defined interval during which specific inputs may be tested to see if they are operating correctly when the area is occupied. The input must be programmed to be included in access tests (determined by the input’s test type).
Access time	The time that a door will remain unlocked after a user has been granted access.
Acknowledge	See “reset”.
Alarm	The state of a intrusion detection system when an input is unsealed and the condition of the area is such that state should be signalled, for example, a door is opened when its area is armed.
Alarm code	The user’s full PIN (used for alarm control and optionally for door control). See also “door code”.
Alarm code prefix digits	The alarm code prefix value in the range one to four enables users to enter a door code (a shorter PIN) for access control. For example, if a user’s full PIN is six digits long (for example, 123456), and the alarm code prefix value is two, then the first two digits are removed for access control, and the user can operate doors by entering only the last four digits of the PIN (for example, 3456).
Alarm control	The control over alarm (arm and disarm) functions.

Alarm group

A panel programming concept that defines a group of areas, functions and menu options. Alarm groups are assigned to users, RASs, or door readers, to define what areas can be controlled and what functions can be performed by that user, or from that device. An alarm group can also be assigned to certain input types such as key switches.

Alarm reporting

A procedure to transmit (via Ethernet, dialler, or other means) alarm events or other events to a remote monitoring company by means of a set of rules called a protocol.

Anti-passback

Anti-passback affects the ability of users to move from one region to another. Entering a region twice in succession is either not possible (hard anti-passback), or will only result in an event being logged in the history log, reported to the printer and to management software (soft anti-passback).

Also see “Privileged”.

Note: This functionality applies only to doors or readers connected to an Intelligent Access Controller.

Area

A logical grouping of input devices that are armed and disarmed simultaneously.

Area group

A Challenger system can have 99 areas, so area groups are used to help manage them. There can be 255 area groups.

Area search

Area search is a process by which a person must ensure that a facility is safe as part of the disarming process.

Armed

See “secure”.

Arming station (RAS)

A remote arming station (RAS) is a device that provides a user interface for security functions for areas or for access points (doors). The RAS may be an LCD keypad, or any other device that can be used to perform security functions such as arm or disarm, open doors, and so on.

Card

A portable device (card or fob) that holds information to identify a user to the Challenger system. The information to identify a user can be stored in a chip (smart card), on a magnetic strip, a bar-code, a Wiegand card, or in biometric data such as a fingerprint.

Card only

The “card only” user flag is enabled for users when you want non-Tecom format cards such as credit cards, financial institution cards, and so on, to be programmed as users, and you want to use only the card and not the PIN.

Note: This functionality applies only to doors or readers connected to an Intelligent Access Controller.

Central station

See “remote monitoring company”.

CID

Ademco Contact ID alarm reporting format.

Computer event

Event-driven mode of IP connection (UDP/IP) to a management software computer.

In event-driven mode, the Challenger panel reports events only as they occur in order to minimise network bandwidth requirements.

Computer polled	Polled mode is typically used for RS-232 or USB connection to a management software computer. It can also be used for IP connection (TCP/IP). Polled mode typically consumes greater bandwidth than event-driven mode. However this can be useful for panels that deliver little event-driven activity. Some networks require a certain amount of activity in order to maintain an active communications path.
Console	See "arming station".
Console warning	Same as keypad buzzer.
DGP	Data Gathering Panel. A DGP expands the capacity of the Challenger system.
Dialler	An electronic device that allows the intrusion detection system to transmit alarms and other events to a remote monitoring company via telephone lines. Can also be used to perform sending and retrieval of access control data with management software.
Disarmed	See “access”.
Door code	An optional version of the user’s PIN shortened by the number of digits specified in the alarm code prefix. The door code is used for access control (for example, to open a door) without revealing the entire PIN used for alarm control.
Door contact	A magnetic contact used to detect if a door or window is opened.
Door control	The control over door functions.
Door group	A panel programming concept that assigns a group of doors to a user in order to allow access at those doors. Access to each door in a group may be restricted via a time zone.
DOTL	Door open too long. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Dual custody	The term “dual custody” is used in the following ways: • If the Challenger system option “Dual Custody Code Programming” is enabled, then two users are required to authenticate before access is granted to menu option 14, Program Users. • If the “dual custody” user flag is enabled for a user, the user will always require a second valid user authentication in order to perform an alarm or access control function at a door or lift connected to an Intelligent Access Controller (doors or lifts 17 to 64 and 81 to 128). • If a RAS connected to an Intelligent Access Controller (doors or lifts 17 to 64 and 81 to 128) is designated as either an “IN reader dual custody” or “OUT reader dual custody”, then two users are required to authenticate in succession in order to unlock the door.

Duress	A situation where a user is being forced to breach the system security (for example, forced at gunpoint to open a door). The duress facility allows a signal to be activated (for example, notification to a remote monitoring company) by the user. See also “keypad duress”.
Egress	Exit, or request to exit (RTE)
Egress input	An input that is programmed to request that a door be briefly unlocked. For example, an egress button is provided inside a doorway to allow users to exit without using a door reader. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Egress time zone	When the egress time zone is valid, a user may press the egress button and the door will unlock. **Note**: This functionality requires the use of an Intelligent Access Controller.
End-of-line resistor	See EOL resistor
EOL resistor	End-of-line resistor used to detect the electrical state of zone input circuits.
Event flag	A signal activated by an input condition, area condition, system status, or fault condition, door command (on doors 1 to 16 on LAN1 and doors 65 to 80 on LAN2), or shunt condition. Event flags are typically used to activate relays or as macro inputs.
Extended access time	A programming option in Intelligent Access Controllers that provides a user with the “long access” user flag enabled to have longer than normal time for a door to unlock. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Extended shunt time	A programming option in Intelligent Access Controllers that provides a user with the “long access” user flag enabled to have longer than normal time for a door to be shunted. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Floor group	A panel programming concept that assigns a group of floors to a user in order to allow selection of those floors when accessing a lift reader. Access to each floor in a group may be restricted via a time zone.
Fob	A type of smart card. See “card”.
Forced arming	Allows areas to arm regardless of any unsealed inputs that may subsequently cause an alarm.
Forced door debounce time	Forced door debounce time delays the generation of a forced door alarm for the specified interval. It caters for certain locks that may cause erroneous forced door reporting. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.

Guard	The term “guard” is used in the following ways: • If the “guard” user flag is enabled for a user, the guard cannot unlock a door without being accompanied by another valid user. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller. • The term “guard” is also used in reference to “guard failed to check in” alarms, which can be generated by means of user category 7.
Hard time zone	See time zone
History	A list of past intrusion detection and access control events stored in memory which can be viewed on an LCD RAS, sent to a printer, or retrieved to a management software computer.
Hold-up alarm	A (silent) alarm that is triggered by a hold-up button. Normally it will not trigger any siren, only send a message to a remote monitoring company.
Holiday	A specified date (or range of dates) during which typical users are denied access during times that they would normally be permitted access.
Holiday type	Functionality to enable access to be granted to certain users during one holiday type, but not necessarily to another holiday type. Each holiday must have at least one type assigned.
In reader	A reader (RAS) that provides entry to a region through a door. The in reader is accompanied by an out reader that provides exit from the region through the door. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
In reader region	When a valid card or PIN is entered at the door’s in reader, the number of the region that the user is entering into is recorded against the PIN. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Input	Also called zone input. An electrical signal from a security device (input device) to the intrusion detection system. Each input device is identified by a system name (for example “INPUT1”), and optionally by a custom name (for example “Reception Holdup Button”).
Input tamper	The Challenger system is typically configured to monitor the state of its zone input circuits (4-state monitoring). Input tamper alarms are generated when the circuit indicates an open-circuit or a short-circuit condition.
Input test	Input test is a defined interval during which a selected input can be tested (toggled from sealed to unsealed and then back to sealed) to verify that the panel correctly identifies the states.
Input type	The input type determines exactly how an input will function when its area is armed or disarmed. Most input types require an area, but some input types that affect the status of areas need alarm groups.
Installer	A person who installs and services security equipment.
Intelligent Access Controller	Four-door or Four-lift DGPs.

Intrusion detection	Electrical detection devices (called inputs) are connected to the Challenger panel or a DGP. Based on the type of device and whether the device’s location (called area) is armed or disarmed, the device triggers an alarm when something activates it. For example, the device might be a reed switch that detects a door being opened when the area is armed. An alarm typically triggers a siren and flashing light to operate, and sends a message to a remote monitoring company.
Isolate	The device is inhibited from reporting alarms. It is excluded from functioning as part of the system.
IUM	Intelligent User Memory. IUM users can have 10-digit PINs and up to 48 bits of raw card data). All Challenger users are IUM users.
Key switch	A device using a key-operated switch to arm or disarm areas.
Keypad	A RAS with buttons to input data.
Keypad duress	When enabled, a duress code (user’s alarm code + 1) can be entered on a keypad to activate a duress alarm. Keypad duress is enabled or disabled in Alarm Groups.
LAN	The term “LAN” is used in the following ways: • The system’s two RS-485 data busses (LAN 1 and LAN 2). • The Challenger panel may be connected to a computer via LAN (local area network) or WAN (wide area network).
Local alarm	An alarm that is reported only within a building, and typically occurs when an area is disarmed (occupied). The circumstances that cause a local alarm can be checked and rectified by personnel on site and it is therefore unnecessary for the alarm to be relayed to a remote monitoring company. Certain input types can generate a local alarm during access (disarmed) times, and can report to remote monitoring company during secure (armed) times.
Logic equation	A logic expression that combines macro inputs in a specific manner. The result of a logic equation produces the macro action.
Long access	The “long access” user flag is enabled for users who need to have longer than normal time for an Intelligent Access Controller’s door to unlock. See “Extended access time”. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Low security time zone	When a RAS’s low security time zone is valid, then either a card or a PIN can be used to open a door. When the time zone is not valid and “Card and Code” is set to YES, then both card and PIN are required to open a door. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Macro input	An event flag or an output that is used in a logic equation. Each macro input is an event flag or output.
Macro logic program	A set of rules that is created by macro inputs, logic equations, and macro outputs.

Macro output	A macro output holds the result of a logic equation. The macro output can have a timing element. Macro outputs trigger event flags or inputs.
Management software	A Challenger system may be programmed and operated via Security Commander management software on a graphical interface.
Operator	Customer staff member or installer who has login rights to system management software.
Out reader	A reader (RAS) that provides exit from a region through a door. The out reader is accompanied by an in reader that provides entry to the region through the door. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Out reader region	When a valid card or PIN is entered at the door out reader, the number of the region that the user is exiting from into is recorded against the PIN. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Override time zone	A door can be programmed with an override time zone that, when valid, automatically keeps the door unlocked. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Perimeter area	An area that contains entry/exit inputs on the perimeter of the premises.
PIN	Personal Identification Number—A number given to, or selected by, a user that identifies the user to the Challenger system.
PIR	Passive Infrared detector. A security device used to detect intruders in a certain part of an area or premises.
Poll	An inquiry message continually sent by the control panel to DGPs and RASs. Polling allows the remote unit to transfer data to the control panel.
Prefix digits	See “Alarm code prefix digits”
Privileged	If the “privileged” user flag is enabled for a user, then anti-passback functionality does not apply to the user (for regions 0 to 199). **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
RAS	Remote arming station. See “arming station”.
Reader	A device (RAS) used for access control that can read magnetic stripe or proximity cards to authenticate the user.
Region	A defined access control area having intelligent doors acting as boundaries. Regions are used by the anti-passback functions to keep track of users. The system can deny access to a card or PIN belonging to a user when the user is already assigned to the region. A region can also keep a count of users in order to activate a macro logic program when a certain value is reached. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Relay	Relay or output from the panel or a relay controller.

Relay controller	A PCB module that connects to the panel or a DGP to provide additional relay or open collector outputs.
Remote monitoring company	A company that monitors whether an alarm has occurred in a intrusion detection system. A remote monitoring company is located away from the building or area it monitors. Also known as “central station”.
Reporting	See “alarm reporting”.
Reset	An authorised user typically must enter a PIN at the keypad to reset (acknowledge) an alarm.
Retrieve	To transfer records from a control panel to a management software computer.
RTE	Request to exit, egress.
Sealed	The input is not activated, for example when a door is closed.
Secure	The state of an area when it’s armed. The condition of an area when it should be vacant and the intrusion detection system has been set so that detected activity generates an alarm. Opposite of “access”.
Secure test	The secure (armed) test is a defined interval during which specific inputs may be tested to see if they are operating correctly when the area is unoccupied. The inputs must be programmed to be included in secure tests (determined by the input’s test type).
SecureStream	Short for SecureStream IP Receiver, an Internet protocol (IP) alarm receiver designed for the Challenger panel alarm network.
Security Commander	Windows-based system management software for Challenger.
Send	To transfer records from a management software computer to a control panel.
Shunt	A procedure that inhibits an input from generating an alarm when unsealed. For example, shunts stops a door generating an alarm when opened for a short time.
Smart card	See “card”.
Soft time zone	A time zone that is active when a relay is active
STU	Subscriber Terminal Unit
STU port	The Challenger PCB’s serial (J15) port.
Tamper	Indication that a security device may have been interfered with. Some devices such as panels and DGPs have tamper switches to detect if they have been opened or removed from their mounting. See “input tamper”.
Tecom IP Receiver	An Internet protocol (IP) alarm receiver designed for the Challenger panel alarm network.
Time and attendance	An LCD RAS connected to an intelligent controller can be used as a time and attendance reader (it generated time and attendance transactions).

Time zone	A time zone is a means of making certain Challenger functionality conditional. ‘Hard’ time zones are valid between defined start and end times on selected days. Soft time zones are valid when a relay (output) is active.
Timezone	See time zone
Total disarm area	The system can be programmed so that one or more areas can have overriding control over the alarm functionality for designated inputs in another area. This functionality is used, for example, to prevent a 24-hour input type from going into alarm when it’s not needed.
Trace user	The “trace user” user flag is enabled for users when you want to be able to trace the user’s operation of an Intelligent Access Controller’s doors or lifts. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Unsealed	The input is activated, for example, when a door is opened.
User	Someone with a PIN and/or a card who can operate the Challenger system (for example, to unlock a door).
User category	User categories provide timing functionality for specific areas.
User flag	Options on a user record that controls how the system operates with respect to the user. User flags are dual custody, guard, visitor, trace user, card only, privileged, and long access. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
User record	A record containing (at least) a user's PIN or card number to identify the user to the Challenger system.
Vault	An area or area group that, when armed, will automatically arm other areas after a specified time.
Visitor	If the user flag “visitor status” is set to YES the user must be accompanied by a non-visitor user. **Note:** This functionality applies only to doors or readers connected to an Intelligent Access Controller.
Zone input	See “input”.

Index