Challenger*Plus* Administrators Manual

P/N MAADMN-TS-CHPLUS • REV 2.1 • ISS 10JAN25

Trademarks and patents

The Challenger name and logo are trademarks of KGS Fire and Security Australia Pty Ltd.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

Made in China by KGS Safety System (Hebei) Co., Ltd.
No. 80, Changjiang East Road, QETDZ, Qinhuangdao, Hebei, P. R. China 066004

Imported by KGS Fire and Security Australia Pty Ltd
Suite 4.01, 2 Ferntree Place,
Notting Hill, Victoria, 3168, Australia

Product warnings and disclaimers

THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. KGS FIRE AND SECURITY AUSTRALIA PTY. LTD. CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY “AUTHORIZED DEALER” OR “AUTHORIZED RESELLER”, IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL FIRE AND SECURITY RELATED PRODUCTS.

For more information on warranty disclaimers and product safety information, please check https://aritech.com.au/aritech-product-warning/ or scan the QR code.

ACMA compliance

Contact information

For contact information, see www.aritech.com.au

Content

Important information

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.

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Aritech 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 Aritech 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 Aritech 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, Aritech assumes no responsibility for errors or omissions.

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 Challenger*Plus* control panels. The product name “Challenger” will often be used in this manual for Challenger*Plus*.

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).

Refer also to other Challenger*Plus* manuals in the suite:

- The *ChallengerPlus Installation and Quick Programming Manual* is for installation technicians to install and commission a Challenger panel.
- The *ChallengerPlus User’s Manual* is suitable for most users of the Challenger system to perform everyday tasks.
- 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”).

Notes:

- The permissions assigned to you may not allow you to do everything described in this manual. You may not be able to see all menu items described in this manual.
- A qualified service person, complying with all applicable codes, should perform all required hardware installation.

Chapter 1
Introduction

Summary

This chapter provides an introduction to the Challenger system.

Content

Welcome to the Challenger system

The *Challenger* integrated intrusion detection and access control panel is widely accepted as a versatile, high-quality, Australian-designed product. Challenger's customisable design makes it the benchmark for intrusion detection (alarm) and access control systems.

The Challenger panel is the heart and soul of the Challenger intrusion detection 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 following tools:

- LCD RAS: Initially the Challenger system must be programmed using a remote arming station (RAS) fitted with a liquid crystal display (LCD) screen and keypad. The RAS's text-based user interface provides a menu that is numbered for rapid access. This manual describes how to program and operate a Challenger system by means of a RAS.
- Management software: A Challenger system that is configured and programmed to be accessed via management software (such as Security Commander) may be programmed and operated via the management software on a graphical interface. Any changes to the Challenger system made via management software must be sent to the Challenger panel before they take effect.

This manual is a reference for the Challenger operations and programming that can be done via RAS. Use management software for advanced operations and programming, and refer to the documentation provided with the management software for assistance.

Note: If management software is used to program a Challenger panel, to change user data or access control data, or used to retrieve a panel's programming, the management software becomes the *primary* location for the panel's data, and the panel becomes the secondary location. In other words, keep track of where the 'correct' version of Challenger data is stored. As administrator you are responsible to avoid loss of data, errors in data, or uncertainty about the validity of data.

A Challenger system might be managed locally from an LCD RAS or via a locally-connected management software computer (Windows computer). Alternatively, the system might be managed remotely via management software computers.

In an Enterprise-wide intrusion detection and access control system, thousands of Challenger systems can be programmed, controlled, and monitored by hundreds of operators working on management software computers in remote locations. Refer to the documentation provided with the management software for details.

Your Challenger system has been programmed to meet your specific requirements. Therefore, not all of the features described in this manual may apply to your system. Also, some of the features described in this manual will not be visible to all users (see “What is a user?” on page 11). Your system may have extra features or equipment installed. The programming instructions for extra equipment are supplied separately.

Testing your system

It is important that you regularly test your Challenger system to ensure that all installed equipment is operating properly.

You may have a technician operate your Challenger system locally or remotely to test and service your intrusion detection system. There are various tests that can be used to ensure your system is working correctly. We recommend that you discuss with the technician the testing processes you can perform to check your system, and its ability to report to your remote monitoring company (if applicable).

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 REPORTS. Refer to the *ChallengerPlus Programming Manual* for maintenance recommendations.

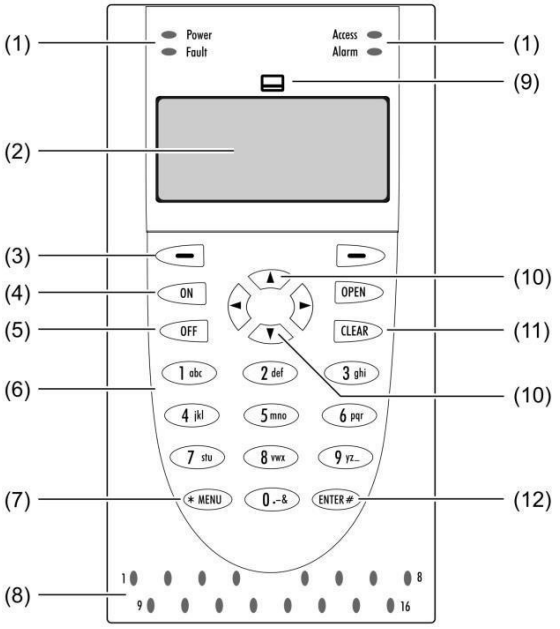
Challenger user interfaces

A Challenger system typically has at least one LCD RAS connected to a LAN (RS-485 data bus). The LCD screen plus keypad provides a text-based user interface for programming and operating the Challenger system. Up to 32 RASs may be connected to the Challenger LANs (depending on Challenger model).

A RAS with a keypad and liquid crystal display (LCD) screen (or a touch screen) enables authorised users to enter a series of numbers called a “code”, in order to perform functions such as accessing the Challenger’s menus, or to open doors.

The CA111x models of the LCD RAS are used in this manual for illustrations and keypad depictions. The CA1116 model shown here (with cover removed) includes a four-line LCD screen and an integral card reader. Figure 1 on page 4 indicates the locations of various controls on the CA1116 RAS.

Figure 1: Details of CA1116 RAS



(1) Status LEDs.

(2) LCD screen.

(3) Multi-function key (adjusts automatically to find area or provide quick control of automation zones)

(4) Press the On key after entering your PIN to tell the Challenger system that you want to arm your areas. (Some arming stations have a # key instead of an ON key).

(5) Press the Off key after entering your PIN to tell the Challenger system that you want to disarm your areas. (Some arming stations have a * key instead of an OFF key).

(6) Press a numeric key to enter numbers, and for entering text when programming user names.

(7) Press the Menu* key to display the menu login prompt; backspace to correct an error; or to scroll backwards in the menu. (Some arming stations have only a * without the word “menu”).

(8) Area LEDs.

(9) Card reader icon (applies to CA1115 and CA1116 models).

(10) Press the up arrow and down arrow keys to scroll through menu options. (Some arming stations have a NEXT key to display additional text).

(11) Press the Clear key to exit the current function or operation and return to alarm control prompt. (Available on some arming stations only).

(12) Press the ENTER key when information is to be processed (similar to the Enter key on a computer); or to scroll forwards in the menu. (Some arming stations have a # instead of the ENTER key).

The LCD screen

Messages are displayed on the liquid crystal display (LCD) screen on the keypad or on a touch screen. These messages guide you through the functions of the Challenger system, such as identifying problems, the procedures necessary to rectify problems, programming functions, and other menu options. The display might also show information you have entered on the keypad. The second line of the display shows instructions and the characters you enter on the keypad.

Welcome screen

A RAS's LCD screen displays messages about the state of the Challenger system and to help navigate the menu options (subject to permissions). The display might also show information you have entered on the keypad.

Figure 2: Default LCD welcome screen

The welcome screen indicates that the Challenger system is ready to receive commands. The top line is a configurable custom message, such as the default time and date, or other text, such as the company name.

Note: Images of LCD screens used in this manual are for illustration only and may not match actual RAS LCD screens.

In some instances there is insufficient space to display all the text being presented (for example, a list of areas in your building). LCD RASs that have small displays (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 text rotation begins after a configurable delay, and scrolls at a configurable speed (this functionality is not applicable to TS0004 or TS0210 LCD RASs).

The bottom line displays "Code" to indicate that the Challenger system is ready to accept a user's personal identification number (PIN), also called a code. The bottom line may also display instructions and the characters you enter on the keypad (except for PINs, which are shown as '*' characters).

Area LEDs

RASs have up to 16 area LEDs that can be used to indicate the state of the system's areas. Areas 1 to 16 are mapped to the RAS's area LEDs by default, but can be reassigned by the installer as needed.

When the CA111x RAS cover is open or removed, 16 LEDs are visible at the bottom of the RAS. Each LED represents an area, and the indications are as follows:

- The LED illuminates when its corresponding area is armed (secure).
- The LED flashes slowly when a fault is detected, or when an alarm occurs, in disarm (access).
- The LED flashes quickly when a fault is detected, or when an alarm occurs, in arm (secure).

CA111x status LEDs

CA111x RASs have four status LEDs above the LCD screen. The indications are as follows:

- **Power**—illuminates when the RAS is powered.
- **Fault**—flashes when there is a system fault (i.e. comms fault, RAS fault, DGP fault, battery test fail, or hardware tamper).
- **Access**—flashes once when a card is badged at CA1115 or CA1116 RASs (subject to Valid Card Flash programming).
- **Alarm**—flashes when there is an access alarm, a 24-hour alarm, or a secure alarm.

TS0804 system fault LEDs

TS0804 RASs have system fault LEDs that indicate as follows:

- **Comms**—illuminates if there is a failure in the communications between the Challenger panel and a remote monitoring station.
- **RAS**—illuminates if a remote arming station is offline.
- **DGP**—illuminates if an access controller or data gathering panel is offline.
- **Battery**—illuminates if the auxiliary battery power is found to be low after mains power is lost.

TS0804 system alarm LEDs

TS0804 RASs have system alarm LEDs that indicate as follows:

- **Access**—illuminates if an alarm has occurred in an area that is occupied and the intrusion detection system has been set to allow normal access.
- **24 Hr**—illuminates if an alarm has occurred in an area where an input device has been programmed for 24 hour monitoring.
- **Secure**—illuminates if an alarm has occurred in an area that is secure (armed).
- **Tamper**—illuminates if an alarm has occurred due to tamper.

Internal beeper

The RAS's beeper provides a number of indications:

- A short beep indicates that a valid card is presented at a reader or a key is pressed on a keypad. The beep may be followed by two beeps to indicate that access has been granted (for example, to open a door).

- Seven short beeps indicates that a PIN or card is not valid at the particular RAS or at the particular time, or that the area you are attempting to arm has an input that is unsealed or in alarm.
- A continuous tone indicates that an input test is being performed.
- Continuous beeping indicates that one or more inputs are in local alarm.
- Your Challenger system may be programmed so that the RAS beeps whilst an entry timer, exit timer, or warning timer is running.

TS1001 Touch Screen RAS

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.

Using the keypad

Use the following steps to access the menu when the “Code” prompt is displayed on the bottom line of the LCD screen.

In the following example, the system is configured to display the time and date instead of the default message “There Are No Alarms In This Area”.

```
14:01 30/08/2018
Code:
```

1. Press [MENU*].

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

2. Press nnnn (where nnnn is your code), and then press [ENTER] to display the user menu prompt.

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

3. From the user menu prompt, you can now select the menu option you need (see Figure 1 on page 4), or press [0] [ENTER] to exit. Alternatively, press [ENTER] (or the RAS’s down button, if applicable) to view the available user menu options in sequence.
4. When finished, press [0] [ENTER] or [CLEAR] to exit the menu.

Note: After a few minutes of inaction, the Challenger system automatically exits the menu and returns to the “Code” prompt. However, we recommend that you press [0] [ENTER] or [CLEAR] to exit the menu when you are finished, in order to prevent unauthorised use (that would otherwise be logged against your code).

The following keys are used to move between menu options:

- Press [ENTER] to scroll forward one menu option.
- Press [MENU*] to scroll backward one menu option.
- Press the menu number and press [ENTER] to jump directly to a menu.
- Press [0] [ENTER] or press [CLEAR] to exit the menu.

To program a value, such as a number or amount, enter the value and press [ENTER]. The information will be saved. Press [ENTER] to display the next option.

To program a YES/NO option, press [ENTER] to accept the display or press [MENU*] to toggle between YES and NO. Press [0] [ENTER] to skip options.

Displaying input names

Input devices are identified by a number and (optionally) a name programmed by the installer. The name is useful to determine the location of an input device that is unsealed or in alarm.

Your Challenger system may be programmed to display inputs by their number, along with their name (Figure 3 below).

Figure 3: Input name displayed

Alternatively, your system might be programmed to display a list of input numbers (Figure 4 below).

Figure 4: Input numbers displayed

In this case, enter an input number, and then press [ENTER] to display the input's name.

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 (see Figure 1 on page 4) 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 (Figure 1 on page 4, item 3) to begin.

Figure 5: Area search prompt

```
Area Search is ,(*)−End
```

3. Use the RAS keypad to enter a search character or string, as described in “Entering text via RAS” below. 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.

Entering text via RAS

A RAS keypad can be used to create or edit text, such as user names or inputs. The RAS’s numbered keys can produce both text and numerals, as listed in Table 1 on page 10. For example, press [2] for “D”, press [2] [2] for “E”, and so on. For example, the initial RAS display for input 1 is shown below (the name is blank).

```
00001:
(1)−Edit
```

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

```
00001: ,(*)−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 1: Key presses to produce characters

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 and you want to completely delete it, use the following steps.

```
00001: 10 Ferntree Place, front door
PIR (1)−Edit
```

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

```
00001: 10 Ferntree Place, front door PIR ,(*)−End
10 Ferntree Place, front door PIR
```

Press [0] to replace the first character with a “.” (see Table 1 above).

```
00001: 10 Ferntree Place, front door PIR ,(*)−End
.10 Ferntree Place, front door PIR
```

Press * to delete all characters and save the programming.

Using the menu

The Challenger system’s user menu has 24 options for use by authorised users, administrators, or installers. The user menu is described in detail in Chapter 3 “Menu reference” on page 19.

Note: A menu option will be visible to you only if allowed by the alarm group assigned to you and to the alarm group assigned to the particular RAS that you are using.

What is a user?

A user is someone with a PIN and/or a card who can operate the Challenger system. It helps to think of users as three main types:

- **Users**: Users can typically arm or disarm the intrusion detection system (called *alarm control*), handle alarms, or open doors (called *access control*). User tasks are described in the *Challenger User Manual*.
- **Administrators**: In addition to a user's role, administrators can add users and perform other administrative tasks, as described in this manual.
- **Installers**: Installers (or alarm technicians) typically install, program, and maintain the Challenger system. Installer tasks are described in the *ChallengerPlus Programming Manual*. Some tasks (such as testing inputs) may be performed by installers instead of administrators. These tasks are described in this manual.

The differences between types of users is determined by what they can do (arming and disarming the system, and by accessing the Challenger menu) and where they can go (by opening doors or accessing floors via a lift).

- A user's ability to arm and disarm the system and to access the Challenger menu is determined by assigning an alarm group to the user. Refer to the *ChallengerPlus Programming Manual* for details about alarm groups.
- A user's ability to open doors is determined by assigning a door group to the user.
- A user's ability to access a floor via a lift is determined by assigning a floor group to the user.

Codes

A PIN (or user code) is a series of 4 to 10 digits that uniquely identifies you to the Challenger system. Your Challenger system may be programmed so that you can use your PIN to arm and disarm the system and to open doors.

Alternatively, your system may allow the use of a *door code* to open doors, and a *duress code* to send a message to the alarm monitoring company. These terms are explained in the *ChallengerPlus Users Manual*.

This page intentionally left blank

Chapter 2
Administrator tasks

Summary

This chapter describes the tasks that a user with administrator privileges would typically perform via a Challenger RAS. These administrator tasks are in addition to tasks such as arming, disarming, and so on, which are described in the *ChallengerPlus User Manual*.

Content

Testing input devices

Testing of Challenger devices may be performed by Challenger system administrators and/or by installers, depending on the situation. In addition, your system may be programmed to initiate tests automatically when arming or disarming the system.

Note: “Automatic test” actually means to automatically start a test interval during which you can test inputs by, for example, opening and closing a door to verify that the Challenger system correctly identifies the input’s change of state from sealed to unsealed and then back to sealed.

Overview of input testing

Input devices are the various items such as passive infrared (PIR) detectors, switches, buttons, and so on, that can indicate a change of state in the Challenger system. The system can recognize input states of sealed and unsealed, and optionally open and shorted (when input tamper monitoring is used).

Testing of inputs involves monitoring the state of the input whilst changing its state from sealed to unsealed, and then back to sealed. This is typically done by, for example, opening and closing a door and then checking the Challenger system to verify that the change was correctly reported.

Being highly configurable, the Challenger system contains a number of testing options to suit a variety of applications. For example:

- You may need to test individual inputs on an ad hoc basis when a device appears to be faulty. See “Option 12 Test Input” on page 28.
- The system may need to be tested periodically in accordance with Australian Standard AS2201.1.
- High security applications like banks may require particular inputs (for example, hold up and suspicion buttons) to be tested in access mode at the start of every day, or tested within a specified number of days via a timer.
- Inputs can be assigned a timer, which is reset each time the input is successfully 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 is generated.

Each input must be programmed for appropriate testing options and the system must be programmed with an appropriate system test mode. In order to conduct tests and interpret reports, you need to understand how certain terms are used. Refer to the Glossary for details.

Conducting an access test

Access testing is typically used for alarm inputs and cameras that you need to test as soon as the area is disarmed. For example, to enable you to test a hold-up button immediately after disarming the area.

If your system contains areas configured as vaults, 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.

Your system may be programmed to automatically go into access test mode when disarming areas that contain inputs configured for access testing. In such a case, the RAS beeper sounds during the access test time, and the LCD screen indicates that the access test is running (Figure 6 below).

Figure 6: Access test RAS display

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). The input (for example, a hold-up button) is disabled during any access test on areas assigned to it.

The area is disarmed after one of the following occurs:

- The access test is cancelled by the user.
- The required inputs are tested (toggled from sealed to unsealed and back to sealed).
- The access test time expires.

An input's access test is recorded as completed if the input is toggled from sealed to unsealed and back to sealed (typically by a technician activating a sensor such as a door contact).

Note: If cameras are programmed to be tested during the access test, and the system is programmed as a financial institution, then the film counters automatically display after the cameras are tested.

Following an access test, you can view the access test report to see if any of the required inputs are untested (see "Access test report" on page 23).

See also "Option 13 Start Auto Access Test" on page 29 for details of how to manually initiate the access testing interval.

Cancelling an access test

From the access test RAS display (Figure 6 on page 15), press [0] [ENTER] [ENTER]. The RAS beeper stops sounding and the selected areas are disarmed.

Conducting a secure test

Secure testing is typically used for inputs that you need to test whilst the area is being armed, for example, to enable you to test a door contact at the end of the day when arming the area.

Your system may be programmed to automatically go into secure test mode when arming areas that contain inputs configured for secure testing. In such a case, the RAS beeper sounds during the test interval, and the LCD screen indicates that the secure test is running (Figure 7 below).

Figure 7: Secure test RAS display

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).

The area is armed after one of the following occurs:

- The secure test is cancelled by the user.
- The required inputs are tested (toggled from sealed to unsealed and back to sealed).
- The secure test time expires.

An input's secure test is recorded as completed if the input is toggled from sealed to unsealed and back to sealed.

Following a secure test, you can view the secure test report to see if any of the required inputs are untested (see "Secure test report" on page 24).

Cancelling a secure test

From the secure test RAS display (Figure 7 above), press [0] [ENTER] [ENTER]. The RAS beeper stops sounding (after the auto test interval expires) and the selected areas are armed.

The secure test takes a little time to finish, in order to give the tested inputs time to reseal.

Using timed input testing

Challenger 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.

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.

A time zone may be defined that excludes certain days (for example, weekends) so that inputs that aren't tested when the facility is closed are not reported as untested.

Refer to the *ChallengerPlus Programming Manual* for details of programming timed input testing functionality.

This page intentionally left blank

Chapter 3
Menu reference

Summary

This chapter provides details of the Challenger user menu options, with the exception of option 19 Install Menu (which is described in the *ChallengerPlus Programming Manual*).

The ability to access a particular RAS menu option is subject to both the user's and the RAS's alarm groups. For example, the RAS may have the permission to display option 19 Install Menu, but if the user does not also have this permission then the option cannot be accessed.

Content

Option 1 Panel Status

Use Panel Status to list:

- Inputs in alarm. The input number is preceded by “A”.
- Inputs in tamper alarm. The input number is preceded by “T”.
- Isolated inputs. The input number is preceded by “i”.
- Unsealed inputs. The input number is preceded by “u”.
- System alarms. For example, DGP tamper.

From the User menu prompt (see “Using the keypad” on page 7), press [1] [ENTER] to display a list of active alarms, tamper alarms, isolated inputs, or unsealed inputs.

No Alarms, Tampers, Isolates, Unsealed.
Press ENTER

Press [ENTER] to exit this option, or press [NEXT] to update the display.

When one or more inputs are in alarm, tamper alarm, isolated, or unsealed, the LCD screen displays the most recent alarm. If you see only numbers and no names, refer to “Displaying input names” on page 8.

Summary On u2, Front Door Contact
NEXT or ENTER

Press [NEXT] or [MENU*] to display additional inputs, if any. Press [ENTER] to exit the option.

Option 2 Input Unsealed

From the User menu prompt (see “Using the keypad” on page 7), press [2] [ENTER] to display a list of unsealed inputs (for example, an open door contact). The LCD screen displays the following information when no inputs are unsealed.

All Inputs are Sealed.
Press ENTER

Note: If the system is configured for input tamper monitoring (four-state monitoring), open circuit and short circuit conditions are also displayed.

Press [ENTER] to exit this option, or press [NEXT] to update the display.

When one or more inputs are unsealed, the LCD screen displays the inputs. If you see only numbers and no names, refer to “Displaying input names” on page 8. The input number is preceded by A if the unsealed input is in alarm, or T if in tamper.

Unsealed On A2, Front Door Contact
NEXT or ENTER

Press [ENTER] to exit the option. Alternatively, press [NEXT] to display additional unsealed inputs.

Option 3 Input In Alarm

From the User menu prompt (see “Using the keypad” on page 7), press [3] [ENTER] to list all inputs that are in an alarm state (but not in local alarm state). You need to know what inputs are in alarm so that the cause of the alarm can be investigated and the alarm reset.

The LCD screen displays the following information when no inputs are in alarm.

No Alarms.
Press ENTER

Press [ENTER] to exit the option. Alternatively, press [NEXT] to refresh the display.

When one or more inputs are in alarm, the LCD screen displays the inputs. If you see only numbers and no names, refer to “Displaying input names” on page 8. The input number is preceded by T if in tamper.

Alarm On 2, Front Door Contact
NEXT or ENTER

Press [ENTER] to exit the option. Alternatively, press [NEXT] to display additional inputs that are in alarm, if any.

Option 4 Input Isolated

From the User menu prompt (see “Using the keypad” on page 7), press [4] [ENTER] to list all isolated inputs to determine which inputs are not operational and need attention.

An isolated input is one which is excluded from functioning as part of the intrusion detection system. It would typically be isolated because it is faulty, and by isolating it you stop it from causing an alarm. See “Option 10 Isolate” on page 27 for details.

The LCD screen displays the following information when no inputs are isolated.

No Isolated Inputs.
Press ENTER

When one or more inputs are isolated, the LCD screen displays the inputs. If you see only numbers and no names, refer to “Displaying input names” on page 8.

Isolated On 2, Front Door Contact
NEXT or ENTER

Press [ENTER] to exit the option. Alternatively, press [NEXT] to display additional isolated inputs, if any.

Option 5 History

From the User menu prompt (see “Using the keypad” on page 7), press [5] [ENTER] to display past events of system history, including alarms and access to the menu. It can help you determine events such as the time that an alarm occurred, the time it was reset and who reset it, the time the system was disarmed in the morning, and so on.

```
1−Alarm Events 2−Log Only Events
Option:
```

Press [1] [ENTER] to display alarm events currently held in the panel’s memory.

```
13:49 26/11 Menu Entered at Console 1 >
1−Scan, 0−Exit
```

The display indicates the most recent event. A > character at the end of the line indicates that the text does not fit on the LCD screen. Press [1] to shift the text sideways to see more, and repeat as needed. A * character at the start of the line indicates that the event is an alarm activation.

Press [ENTER] to view earlier events, or press [NEXT] to view later events.

The above example shows:

- The time of the event in hours and minutes (HH:MM).
- The date of the event as day and month (DD/MM).
- The type of event, for example, Menu Entered.
- The location of the event, for example, Console (RAS) 1.
- The user’s number and name (if applicable). In this case, press [1] to shift the text sideways to see the additional text.

Enter [2] and press [ENTER] to display events currently held in the panel’s memory that are not reported to the monitoring station but sent to local printer or computer (for example, access granted at door).

Option 6 Test Report

Inputs can be programmed to be included in either an access test or a secure test. This means that a predefined timer starts running, and during this interval the system looks for the input’s state to be toggled from sealed to unsealed and back to sealed (typically by a technician activating a sensor such as a door contact). See “Testing input devices” on page 14.

If an access test or a secure test (interval) has occurred and any inputs that are programmed to be included in the test have not been toggled (i.e. tested), they will be available for viewing via the Test Report option.

From the User menu prompt (see “Using the keypad” on page 7), press [6] [ENTER] to display the current testing status of inputs configured for access or secure testing.

```
Test Report 1−Access 2−Secure
Option:
```

Press [1] [ENTER] to display the results of inputs tested during access (disarmed) tests. See “Access test report” below.

Enter [2] and press [ENTER] to display the results of inputs tested during secure (armed) tests. See “Secure test report” on page 24.

Alternatively, press [ENTER] to exit this option.

Access test report

This function displays the results of the access (disarmed) test, which can be performed on specific inputs and cameras to see if they are operating correctly. The inputs must be programmed to be included in access tests (determined by the input’s test type). The system must be programmed with an appropriate test mode.

From the Test Report menu option, enter [1] and press [ENTER] to display the results of inputs tested during access tests. If all inputs that are programmed to be tested (including 0 inputs) during an access test have been tested, the LCD screen displays the following.

```
No Untested Inputs.
Press ENTER
```

Alternatively, when one or more inputs are untested, the LCD screen displays the inputs. If you see only numbers and no names, refer to “Displaying input names” on page 8.

```
Untested Access On 25, Reception Hold Up
NEXT or ENTER
```

Press [NEXT] to update the list of untested inputs, and to display the remaining inputs in the list (if any).

Press [ENTER] to display the results of camera testing (cameras in area 1 only). If all the cameras that are programmed to be tested (including 0 cameras) have been successfully tested the LCD screen displays the following.

```
All Cameras Have Tested Successfully
Press ENTER
```

Press [ENTER] to exit the option.

Use “Option 12 Test Input” on page 28 to manually test any untested inputs reported.

Secure test report

This option is used to display the results of the secure (armed) test, which can be performed on specific inputs to see if they are operating correctly. The inputs must be programmed to be included in secure tests (determined by the input's test type). The system must be programmed with an appropriate test mode.

From the Test Report menu option, enter [2] and press [ENTER] to display the results of inputs tested during secure tests. If all inputs that are programmed to be tested (including 0 inputs) have been successfully tested the LCD screen displays the following.

```
No Untested Inputs.
Press ENTER
```

Alternatively, when one or more inputs are untested, the LCD screen displays the inputs. If you see only numbers and no names, refer to "Displaying input names" on page 8.

```
Untested Secure On 17, Rear Door Contact
NEXT or ENTER
```

Press [NEXT] to update the list of untested inputs, and to display the remaining inputs in the list (if any).

Press [ENTER] to exit the option.

Use "Option 12 Test Input" on page 28 to manually test any untested inputs reported.

Option 7 Service Menu

From the User menu prompt (see "Using the keypad" on page 7), press [7] [ENTER] to request a service call or to manage connections to a computer in order to program the Challenger system remotely.

The first option displayed is Request Service Technician.

```
1−Request Service
Technician 0−Exit, Menu:
```

The Service menu contains the following options:

- 1—see "Request Service Technician" on page 25.
- 2—see "Disconnect management software" on page 25.
- 3—see "Dial management software" on page 25.
- 4—see "Dial temporary management software" on page 25.
- 5—see "Answer management software" on page 26.
- 6—not applicable to Challenger*Plus*.
- Press [ENTER] to scroll through the options.

- Press [0] [ENTER] to exit this option.

Request Service Technician

Your Challenger system may be configured so that you can send a message to your alarm monitoring company requesting a service technician to contact you.

```
1 Request Service
Technician 0−Exit, Menu:
```

From the Service menu, press [1] [ENTER] to select option 1.

```
1 Confirm Dial
0−Exit, Menu:
```

Press [1] [ENTER] to send a Service Request event to your alarm monitoring company. Alternatively, press [0] [ENTER] to cancel.

Disconnect management software

Use this option to disconnect an active connection that has “Connect on Service” option enabled. If there is more than one enabled path with “Connect on Service” option enabled, then the path with the highest priority is automatically selected.

From the Service menu, press [2] [ENTER] to disconnect from management software. Challenger disconnects and exits the menu.

Dial management software

Use this option to initiate an enabled communication path’s connection to management software (dial the path’s phone number 1 and attempt to connect to the remote service modem). If there is more than one enabled path with “Connect on Service” option enabled, then the path with the highest priority is automatically selected.

From the Service menu, press [3] [ENTER] to dial management software.

```
1 Confirm Dial
0−Exit, Menu:
```

Press [1] [ENTER] to dial phone number 1. Alternatively, press [0] [ENTER] to cancel.

Dial temporary management software

Use this option to enter a temporary service telephone number and initiate an enabled communication path’s connection to management software (dial the temporary service telephone number that you enter, and attempt to connect to the remote service modem). If there is more than one enabled path with “Connect on Service” option enabled, then the path with the highest priority is automatically selected.

From the Service menu, press [4] [ENTER] to select dial temporary management software.

```
'*'–Pause, Phone No:
Ser No:
```

Enter up to 10 digits to program a temporary service telephone number, and then press [ENTER].

```
1 Confirm Dial
0–Exit, Menu:
```

Press [1] [ENTER] to dial the temporary service number. Alternatively, press [0] [ENTER] to cancel.

Answer management software

Use this option to answer dial-in attempts received within the next five minutes (on an enabled communications path).

The “Connect on Service” option is enabled by default for communications path 10–SERVICE, however there can be other paths with the “Connect on Service” option enabled. The enabled path with the highest priority is automatically selected.

Enter [5] and then press [ENTER] to begin the five-minute interval in which the Challenger panel can answers calls.

Option 8 Film Counters

From the User menu prompt (see “Using the keypad” on page 7), press [8] [ENTER] to display the current frame number position on each of the security camera films.

If a camera is fitted with a film out detector and that camera does not have a film in it, the frame count will be displayed as OUT (OUT is removed when film is loaded).

Up to eight cameras can be displayed. A camera position that does not have a camera fitted will display the frame count as ‘--- ’.

A frame count can be from 0 to 9999.

```
Film Counts 1: 0123 2:1077 3:0056 4: ----
Press ENTER
```

Press [ENTER] to see the film counts for cameras 5 to 8. Press [ENTER] a second time to exit this menu.

Option 9 Input Text

From the User menu prompt (see “Using the keypad” on page 7), press [9] [ENTER] to display the names assigned to inputs 1 to 1008.

```
Input: 1, Rear Door Contact
Input No:
```

The LCD screen displays the first input number and its assigned name. If you see only numbers and no names, refer to “Displaying input names” on page 8.

Press [NEXT] or [MENU*] to display subsequent input names. Alternatively, enter the input number and press [ENTER] to display the input’s name.

Press [ENTER] to exit the display.

Option 10 Isolate

You may need to isolate an input to prevent false alarms (possibly due to a faulty input device). A faulty input is typically unsealed, and cannot be sealed. Isolating the input excludes it from functioning as part of the intrusion detection system.

If an input is in an alarm state, then isolating it resets the alarm. After the problem is resolved the input must be de-isolated (see “Option 11 Deisolate” below).

From the User menu prompt (see “Using the keypad” on page 7), press [1] [0] [ENTER]. The LCD screen displays the first unsealed input or the message “All Inputs are Sealed”.

```
Unsealed on 1, Front door contact
Input No:
```

Press [NEXT] or [MENU*] to display subsequent inputs.

Enter the input number and press [ENTER] to isolate that input. If an attempt is made to isolate an input which is already isolated, the request appears as if it is processed but it is not logged in the history and the input remains isolated.

When finished, press [ENTER] to exit this option.

Option 11 Deisolate

An input may have been isolated to prevent false alarms (possibly due to a faulty input device). Isolating the input excludes it from functioning as part of the intrusion detection system (see “Option 10 Isolate” above). After the problem is resolved the input must be de-isolated.

Note: Do not de-isolate the input before checking the circumstances, because de-isolating an unsealed input may cause an alarm.

From the User menu prompt (see “Using the keypad” on page 7), press [1] [1] [ENTER]. The LCD screen displays a list of isolated inputs or the message “All Inputs are De-Isolated”.

```
Isolated on u3, Rear door contact
Deisolate:
```

Press the displayed number of an isolated input and then press [ENTER] to deisolate that input.

Press [NEXT] or [MENU*] to display additional isolated inputs (if any). Select the required isolated input and then press [ENTER] to deisolate that input.

When finished, press [ENTER] to exit this option.

Option 12 Test Input

Use Test Input to start a defined interval (input test time) during which you can test an individual input (even if the input is isolated). The input will not generate alarms while in test.

When you select the Test Input option and enter the input’s number, you can then test the input by manually altering its state (for example, by walking in front of a PIR) and verifying that the system correctly identifies the state. During the test, the keypad buzzer will sound when the input is unsealed.

From the User menu prompt (see “Using the keypad” on page 7), press [1] [2] [ENTER].

```
Test Individual Input
Input No:
```

Enter an input number and then press [ENTER] to display the state of the input and begin the testing interval.

```
SEALED on 6, Loading dock
Press ENTER
```

Unseal the input device and then seal it. When the input is unsealed, open, short, or sealed, the display should indicate the state.

```
UNSEALED on 6, Loading dock
Press ENTER
```

Depending on how your system is programmed for input tamper monitoring (four-state or two-state); the results can indicate the conditions shown in Table 2 below.

Table 2: Input testing results

Input condition	4-state monitoring (default)	2-state monitoring
Sealed	Sealed	Sealed
Unsealed	Unsealed	Unsealed

Input condition	4-state monitoring (default)	2-state monitoring
Open circuit	Open	Unsealed
Short circuit	Short	Unsealed

If the input is not sealed, the RAS emits a continuous tone. When the input is sealed, the display will be updated and the tone will stop. Alternatively, press [ENTER] to stop the tone and return to the previous screen.

Press [ENTER] when finished to exit this option.

Note: If the test is not completed within the input test time (default is 5 minutes), the option is exited.

Option 13 Start Auto Access Test

From the User menu prompt (see “Using the keypad” on page 7), press [1] [3] [ENTER] to initiate a defined interval during which specific untested inputs and cameras (camera count input types) may be tested to see if they are operating correctly when the area is in access (disarmed).

Note: This option may be used regardless of the programmed Challenger system test mode. However, if an access test was automatically run and completed before using this option, then the Test Completed message will display, and no inputs will need to be tested.

The following programming is required:

- The inputs to be tested must be included in access tests (input test types 1, 2, 4, or 5). Camera count inputs must be assigned input test type 0 “No Testing”.
- The access test time programmed by the installer must be sufficient for you to test all the required inputs (default time is 15 minutes).

The RAS beeper sounds continuously during the testing time or until you exit this option.

Access Test, NEXT For Untested
"0"−Cancel:

From the initial screen, press [NEXT] to display an untested input, test the input by unsealing and then sealing it, and press [NEXT] to display the next untested input. Repeat until all inputs have been tested.

If [NEXT] is selected to display any untested inputs, the LCD screen displays the first input number and its assigned name. If you see only numbers and no names, refer to “Displaying input names” on page 8.

Untested Access On 4, Office PIR
NEXT or ENTER

Alternatively, press [ENTER] to proceed to the camera test or the Test Completed/Not Completed display (as applicable).

```
Untested Access On 2, Camera 1
NEXT or ENTER
```

Inputs that are programmed as a camera input types (and assigned to area 1) are also tested.

```
All Cameras Have Tested Successfully
Press ENTER
```

When all inputs that are programmed to be tested (including 0 inputs) during the access test have been tested, or the time allowed for access test has expired, the test will automatically cease and the display will indicate if the test is completed or not completed.

```
Test Completed
Press ENTER
```

Press [ENTER] to exit this option.

Note: If your Challenger system is programmed as a financial institution system, and is programmed to automatically go into access test mode when disarming area 1 (which contains camera film count inputs), then you will see the current film counts for cameras 1 to 4. The LCD screen will resemble the example in “Option 8 Film Counters” on page 26 until you press [ENTER] or the display times out.

If there are any tests not completed, you can again select Start Auto Access Test to finish the testing.

Option 14 Program Users

From the User menu prompt (see “Using the keypad” on page 7), press [1] [4] [ENTER] to manage the user records that are stored in the Challenger panel’s memory. For tasks involving large quantities of users it’s best to use management software such as Security Commander.

Note: Your Challenger system may be configured for dual custody programming, where any user (other than the master user) requires a second user to enter their code before access is granted to this option.

```
1−Delete 2−Display 3−Create 4−Total
Option:
```

The Program Users menu contains the following options:

- 1—see “Delete user” on page 31.
- 2—see “Display user” on page 31.
- 3—see “Create (or modify) user” on page 33.

- 4—see “Total users” on page 37.
- Press [0] [ENTER] to exit this option.

See also “Programming non-Tecom magnetic card formats” on page 37.

We suggest that you record the details of users on the User worksheet (see “Users worksheet” on page 50).

Delete user

From the Program Users menu, press [1] [ENTER] to delete a user.

```
Delete User
User No:
```

Enter the user number and then press [ENTER] to delete the user record. Repeat if needed for another record.

Press [ENTER] again to exit this option.

Note: Unlike previous versions of Challenger panels, you can’t actually delete user 50 from the panel (however, user 50 can be deleted from management software and from 4-Door or 4-Lift Controllers). When you ‘delete’ user 50 from the panel, the user record is voided and not deleted. Doing so can create a user tally that differs between the panel and management software or 4-Door or 4-Lift Controllers.

Display user

From the Program Users menu, press [2] [ENTER] to display a user’s details (assuming that you permissions to view the user).

```
Display User
User No:
```

Note: In the Display user option, you may see prompts to use the [MENU*] key to change a setting. The [MENU*] key is not applicable to this option.

Enter the user number and then press [ENTER] to display the user’s name (if the system is programmed to allow user name files), for user numbers in the range 1 to 2000.

```
2:Your Name is Francis Smith
Press ENTER
```

Press [ENTER] to display the user’s alarm group.

```
2:Alm Grp:12,Manager
Press ENTER
```

Press [ENTER] to display the user’s door group.

```
2:Door Group: 2
Press ENTER
```

Press [ENTER] to display the user's floor group.

```
2:Floor Group: 0
Press ENTER
```

Press [ENTER] to display the first of the user flags (if the system is programmed to display user flags).

```
2:NO − Dual Custody
*−Change 0−Skip
```

Press [ENTER] to display subsequent user flags. Alternatively, press [0] to skip the subsequent user flags.

The user flags displayed in sequence are:

- dual custody
- guard
- visitor
- trace user
- card only
- privileged
- long access

Press [ENTER] to display the user's start time and date.

```
2:Start Date: 00:00 00/00/2000
Press ENTER
```

The default start time and date is 00:00 00/00/2000 and has no effect on the user. If the start time and date is in the future, then the user will be activated at the specified start time and date.

Note: The user's start date is not sent to Four-Door Controllers or Four-Lift Controllers.

Press [ENTER] to display the user's end time and date.

```
2:End Date: 00:00 00/00/2000
Press ENTER
```

The default end time and date is 00:00 00/00/2000 and has no effect on the user. If the end time and date is in the future, then the user will be deactivated at the specified end time and date.

Note: The user's end date is not sent to Four-Door Controllers or Four-Lift Controllers. This option will not remove a user's access rights via a Four-Door Controller or Four-Lift Controller past the end date if they had access rights prior to the end date.

Press [ENTER] to display the user's PIN code (if the system is programmed to allow users other than the master installer to see PIN codes).

```
2:Pin Code: 4346
Press ENTER
```

Press [ENTER] to display the user's card data.

```
2:Card Bits: 27.0.0.0.25.0.6
Press ENTER
```

Press [ENTER] to exit this user record and return to the Display User screen.

Create (or modify) user

In any given Challenger panel, the process of using a RAS to create a new user, or to modify an existing user is very similar. You need to:

- Enter the user number that you want to add or modify (in addition to the default master installer user 50).
- Step though the LCD screens, adding or changing details as you go.
- Press [ENTER] at the end to save the details.

A basic Challenger panel used only for intrusion detection (and not access control) might require only the most basic information such as user number, alarm group, and PIN code. Some Challenger systems allow you to program many other user options, such as:

- The user's name.
- A door group and a floor group defines where the user is allowed to go and at what times of day.
- User flags that further configure how the user's access permissions are handled by the Challenger system.

Some Challenger panels enable you to enter or update a user's card data electronically by presenting the card to the reader (called learning the card data), or by manually entering card data.

From the Program Users menu, press [3] [ENTER] to create or modify a user. Assuming that there is room in the user database, the following screen displays.

```
Create User
User No:
```

Enter the new or existing user number, and then press [ENTER] to program or display the user's name (if the system is programmed to allow user name files), for user numbers in the range 1 to 2000.

```
3:Your Name is Francis Smith
(1)−Edit
```

Enter up to 16 characters of text for the user's name (see "Entering text via RAS" on page 9).

When you've finished entering the name, press [MENU*] [MENU*] to save the name, exit the option, and then to select or change the alarm group.

```
3:*−View, Alm Grp:1−No Access
Alarm Group:
```

Enter the number of the alarm group, and then press [ENTER] to assign the alarm group to the user. Alternatively, press [NEXT] to display a list of alarm groups that you can issue to a user.

Notes:

- You cannot assign an alarm group to a user unless the alarm group has the option "Can this Alarm Group be Assigned to Users" set to YES
- Your alarm group must have all the areas and menu options of the alarm group you wish to assign.

Press [ENTER] to display or change the user's door group.

```
3:Door Group: 0
Door Group
```

Press [ENTER] to display or change the user's floor group.

```
3:Floor Group: 0
Floor Group
```

Press [ENTER] to display or change the first of the user flags (if the system is programmed to display user flags).

```
3:NO − Dual Custody
*−Change 0−Skip
```

If required, press [MENU*] to toggle the programmed value from NO to YES, and then press [ENTER] to display subsequent user flags. Alternatively, press [0] to skip the subsequent user flags.

The user flags displayed in sequence are:

- Dual custody
- Guard
- Visitor
- Trace user
- Card only
- Privileged
- Long access

Press [ENTER] to program or display the user's start time and date.

```
3:Start Date: 00:00 00/00/2000
(1)−Edit
```

The default start time and date is 00:00 00/00/2000 and has no effect on the user. If the start time and date is in the future, then the user will be activated at the specified start time and date.

Note: The user's start date is not sent to Four-Door Controllers or Four-Lift Controllers.

Press [ENTER] to accept the displayed value, or press 1 to edit the hours field.

```
3:Start Date: 00:00 00/00/2000
Hours:
```

Press one or two digits for the hours, and then press [ENTER] to edit the minutes. Repeat for day, month, and then year.

Press [ENTER] to display the user's end time and date.

```
3:End Date: 00:00 00/00/2000
(1)−Edit
```

The default end time and date is 00:00 00/00/2000 and has no effect on the user. If the end time and date is in the future, then the user will be deactivated at the specified end time and date.

Press [ENTER] to accept the displayed value, or press 1 to edit the hours field.

```
3:End Date: 00:00 00/00/2000
Hours:
```

Press one or two digits for the hours, and then press [ENTER] to edit the minutes. Repeat for day, month, and then year.

Note: The user's end date is not sent to Four-Door Controllers or Four-Lift Controllers. This option will not remove a user's access rights via a Four-Door Controller or Four-Lift Controller past the end date if they had access rights prior to the end date.

Press [ENTER] to display or change the user's the user's PIN code (if the system is programmed to allow users other than the master installer to see PIN codes).

```
3:Pin Code: 4346
Code:
```

The minimum PIN code length is 4 digits (5 for financial institutions), plus any value programmed for the alarm code prefix. For example, if your system uses an alarm code prefix value of 2 (digits) then you must program PIN codes of at least 6 digits (4 + 2). Press [ENTER] to learn the card data from a reader.

```
3:Waiting For Card
*− Hist
```

Do one of the following:

- Present a card at the designated card learn reader, and then press [ENTER] to save the card bit data in the user record. See "Learning card data" on page 36.

- Press [MENU*] to use unknown card data from the Challenger panel's history. See "Using data from card history" below.
- Press [ENTER] to manually enter the card data bits. See "Manually entering card data" below.

Learning card data

At the Waiting For Card prompt, present a card at the designated card learn RAS. The LCD screen displays the card bit data.

```
Card Bits: 27.0.0.0.25.0.6
Bits 1:
```

Press [ENTER] to save the card bit data in the user record, and then return to the Create User screen.

Note: The card learn RAS number is programmed in the Challenger panel's System Options. Refer to the *ChallengerPlus Programming Manual* for details.

Using data from card history

At the Waiting For Card prompt, press [MENU*] to display the start of the card history list.

```
No 1 27.0.0.0.25.0.6
* Next, # Enrol
```

Press [ENTER] to save the card bit data in the user record, and then return to the Create User screen.

Alternatively, press [MENU*] to display the next record in the card history list until you find the one you want.

If there are no more records the card history list the following screen displays.

```
End Of History
Press ENTER
```

Press [ENTER] to return to the Create User screen.

Manually entering card data

At the Waiting For Card prompt, press [ENTER] to display the card bits.

```
3:Card Bits: 0.0.0.0.0.0.0
Bits 1:
```

Enter the card bits (raw card data) in format xxx.xxx.xxx.xxx.xxx.xxx.xxx, where each field is a number from 0 to 255. Press [ENTER] after each number to save the data and move to the next field.

When the last field is populated, press [ENTER] to exit this user record, and then return to the Create User screen.

Modifying a user

The process of modifying a user is similar to the process of creating a user, except that each screen will display the previously-programmed values. If the user already has card data that you need to change, you have the option of deleting the card data and learning or manually entering new card data, starting at the Waiting For Card prompt.

```
3:Card Bits: 27.0.0.0.25.0.6
*−Del (1)−Edit
```

Do one of the following:

- Press [MENU*] to completely delete the card data.
- Press [1] to manually edit the card data bit by bit.

```
3:Card Bits: 27.0.0.0.25.0.6
Bits 1:
```

Press [ENTER] to save the card bit data in the user record, and then move to the next bit. When finished entering or accepting card data bits, press [ENTER] to return to the Create User screen.

Total users

You may need to know how many users are stored in the Challenger panel's memory (including the default user 50). For example, if the total number of users is 21, then 20 users have been added, plus the master user 50.

From the Program Users menu, press [4] [ENTER].

```
Total Users 21
Press ENTER
```

Press [ENTER] to return to the User screen.

Programming non-Tecom magnetic card formats

The following procedure must be used to allow non-Tecom format cards such as credit cards, financial institution cards, and so on, to be programmed as users. Your system must be equipped with the appropriate card reader in order to perform this function.

Use the following steps to record the non-Tecom format card enrolment number in the user record:

1. Swipe the card in the reader.
2. If the card is not recognized by the system, an event will be logged in history as "Card/Pin" followed by an enrolment number of up to 10 digits (for example, "Card/Pin 1234512345"). Note the enrolment number, which will be recorded as the PIN code when programming the user.

3. Follow the procedure described in “Create (or modify) user” on page 33, and enter the enrolment number as the PIN code.

If you want the user to use the card but not the PIN code (enrolment number), the following options must be programmed:

- The system must be programmed to display user flags when programming users.
- Set the user flag “card only” to YES when programming the user.

Option 15 Time & Date

From the User menu prompt (see “Using the keypad” on page 7), press [1] [5] [ENTER] to manage the Challenger panel’s time and date settings (for example, to program the daylight savings time start and end dates).

```
Time 1−Display, 2−Set, 3−DST, 4−Correct
0−Exit, Menu:
```

Display

From the Time & Date menu, press [1] [ENTER]. The LCD screen displays the panel’s current time and date settings.

```
Time 14:33:59 23/05/2018 Wednesday
0–Exit
```

Press the [0] or [ENTER] to return to the Time & Date menu.

Set

From the Time & Date menu, press [2] [ENTER]. The LCD screen displays the panel’s current time and date settings.

```
Time 14:33:59 23/05/2018 Wednesday
Hours:
```

Enter the hours in 24-hour format (or accept the current value), and then press [ENTER].

```
Time 14:33:59 23/05/2018 Wednesday
Minutes:
```

Enter the minutes (or accept the current value), and then press [ENTER].

```
Time 14:33:59 23/05/2018 Wednesday
Seconds:
```

Enter the seconds (or accept the current value), and then press [ENTER].

```
Time 14:33:59 23/05/2018 Wednesday
Day of Mth:
```

Enter the day of month (or accept the current value) and press [ENTER].

```
Time 14:33:59 23/05/2018 Wednesday
Month:
```

Enter the month (or accept the current value) and press [ENTER].

```
Time 14:33:59 23/05/2018 Wednesday
Year:
```

Enter the last two digits of the year (or accept the current value) and press [ENTER].

```
Time 14:33:59 23/05/2018 Wednesday
Year:
```

Review the displayed settings and press [ENTER] to save. Alternatively, press [0] [ENTER] to abandon your changes and exit this option.

DST

From the Time & Date menu, press [3] [ENTER] to program the daylight savings time start and end dates).

```
0−Disable, Month 00
Start Sunday:
```

Enter a value in the range 1 to 5 and press [ENTER] to indicate which Sunday in the month daylight savings time begins. The following example shows the LCD screen where a value of 1 is entered.

```
1−First Sunday, Month 00
Start Sunday:
```

If correct press [ENTER] to accept, and then to program the start month.

```
1−First Sunday, Month 00
Start Month:
```

Enter a value in the range 1 to 12 and press [ENTER] to indicate which month daylight savings time begins. The following example shows the LCD screen where a value of 10 is entered.

```
1−First Sunday, Month 10
Start Month:
```

If correct press [ENTER] to accept, and then to program the end Sunday.

```
0−Disable, Month 00
End Sunday:
```

Enter a value in the range 1 to 5 and press [ENTER] to indicate which Sunday in the month daylight savings time ends. The following example shows the LCD screen where a value of 1 is entered.

```
1−First Sunday, Month 00
End Sunday:
```

If correct press [ENTER] to accept, and then to program the end month.

```
1−First Sunday, Month 00
End Month:
```

Enter a value in the range 1 to 12 and press [ENTER] to indicate which month daylight savings time ends. The following example shows the LCD screen where a value of 4 is entered.

```
1−First Sunday, Month 04
End Month:
```

If correct press [ENTER] to accept.

Correct

From the Time & Date menu, press [4] [ENTER] to program a time correction for the Challenger panel's internal clock (if needed).

```
Seconds Correction Per Day: +0
*−Chg, Sec:
```

Enter the value in seconds, press [MENU*] to toggle the + or – factor, for the amount of seconds you need to add or subtract each day, and then press [ENTER].

Option 16 Isolate/Deisolate RAS/DGP

From the User menu prompt (see "Using the keypad" on page 7), press [1] [6] [ENTER] to temporarily exclude from the Challenger system fault or tamper messages (system alarms) that are being generated by an arming station (RAS) or data gathering panel (DGP). This would be used if a RAS or DGP has generated a system alarm or is out of service, and needs to be isolated while awaiting service.

Isolating a RAS or DGP will also reset any system alarm generated by the RAS or DGP. Isolating a DGP will not isolate the alarm inputs on that DGP, but will disable DGP's offline and online reporting.

```
1−RAS, 2−DGP Isolate / Deisolate
0−Exit, Menu:
```

Isolate RAS

From the Isolate/Deisolate RAS/DGP menu, press [1] [ENTER].

```
No RASs Are Isolated
Isolate RAS:
```

Alternatively, if RAS 5 has previously been isolated the display would indicate the following.

```
5,
Isolate RAS:
```

Enter a RAS number and then press [ENTER] to toggle its isolated/deisolated state. For example, press [5] [ENTER] to deisolate RAS 5, or press [6] [ENTER] to isolate RAS 6 and add it to the top line.

The procedures for isolating or deisolating a DGP are the same as for a RAS.

When finished deisolating RASs and DGPs, press the down arrow key or [ENTER] to return to the Isolate/Deisolate RAS/DGP menu.

Option 17 Enable/Disable Service Tech

From the User menu prompt (see “Using the keypad” on page 7), press [1] [7] [ENTER] to enable the service technician’s PIN or card for the programmed service time period, or to cancel the service technician’s PIN or card prior to the expiration of the service time.

Note: This menu is disabled when any areas are armed, unless the system option “Skip Access Check For Service Menu” is enabled.

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

```
0−Cancel, 1−Service In
Option:
```

From the Enable/Disable Service Tech menu, press [1] [ENTER] to enable the service technician for the programmed service time period and to exit to the menu.

If not expired, the programmed service time period may be extended by reactivating the option. Press [1] [ENTER] during the service time period or Service Ending warning to reactivate.

If you need to cancel the service technician’s PIN or card before the service time expires, press [0] [ENTER].

Option 18 Reset Cameras

From the User menu prompt (see “Using the keypad” on page 7), press [1] [8] [ENTER] to reset the film frame count on all security cameras connected directly to the Challenger panel to zero or to change the frame count number on

an individual camera. This would be necessary when you change the film in the camera.

```
Reset Camera Counts "0#"−All
Camera No:
```

Press [0] [ENTER] to reset the film frame count on all security cameras to zero.

Press [n] [ENTER] to display the current film frame count on camera n. Press [ENTER] a second time to return to the Reset Camera screen.

Alternatively, enter a new frame count in the range 0 to 1900 for the selected camera, and then press [ENTER] to return to the Reset Camera screen.

Option 19 Install Menu

Access to the Install menu is typically limited to installers or administrators. Refer to the *ChallengerPlus Programming Manual* if you are an installer or administrator and you need to know details of Challenger system programming.

Option 20 Door and Floor Groups

From the User menu prompt (see “Using the keypad” on page 7), press [2] [0] [ENTER] to program door groups and floor groups.

A door group contains a list of doors and a time zone for each door. A floor group contains a list of floors and a time zone for each floor. The time zone assigned to the door group or floor group restricts user access to the times defined in the time zone. Time zone 0 provides 24-hour access to authorized users.

```
Groups, 1−Doors 2−Floors
Option:
```

Press [1] [ENTER] to program a door group, or press [2] [ENTER] to program a floor group. Alternatively, press [ENTER] to exit this option.

Programming or modifying a door group

We suggest that you record the details of Door Groups on the Door Groups worksheet (see “Door groups worksheet” on page 51).

From the Door and Floor Groups menu, press [1] [ENTER] to program a door group.

```
Door Groups
Group No:
```

Enter a door group number in the range 1 to 255 and press [ENTER].

The LCD screen displays the door group number, four of the possible 128 doors, and each door’s assigned time zone (if ‘**’ displays instead of a time zone

number, then the door is disabled). Pressing * when Enter Door: is displayed scrolls through all 128 doors.

```
Door Grp 1 D1−** D2−** D3−** D4−**
Enter Door:
```

For each door in the door group, enter a door number in the range 1 to 128, and then press [ENTER] to allocate a time zone to the door.

```
Door Grp 1 D1−01 D2−** D3−** D4−**
*−Dis, Tz−D1:
```

Enter a time zone number in the range 1 to 63, and then press [ENTER] to return to the Enter Door prompt.

Alternatively, if you need to disable a door, enter [MENU*] as the time zone and then press [ENTER] to return to the Enter Door prompt.

```
Door Grp 1 D1−01 D2−** D3−** D4−**
Enter Door:
```

We suggest that each time you program or change a door group, you record the details on the Door groups worksheet.

Programming or modifying a floor group

We suggest that you record the details of floor groups on the Floor Groups Worksheet (see “Floor groups worksheet” on page 53).

From the Door and Floor Groups menu, press [2] [ENTER] to program a floor group.

```
Floor Groups
Group No:
```

Enter a floor group number in the range 1 to 128 and press [ENTER].

The LCD screen displays the floor group number, four of the possible 64 floors, and each floor’s assigned time zone (if ‘**’ displays instead of a time zone number, then the floor is disabled). Pressing * when Enter Floor: is displayed scrolls through all 64 floors.

```
Floor Grp 1 F1−** F2−** F3−** F4−**
Enter Floor:
```

For each floor in the floor group, enter a floor number in the range 1 to 64, and then press [ENTER] to allocate a time zone to the floor.

```
Floor Grp 1 F1−01 F2−** F3−** F4−**
*−Dis, Tz−F1:
```

Enter a time zone number in the range 1 to 63, and then press [ENTER] to return to the Enter Floor prompt.

Alternatively, if you need to disable a floor, enter [MENU*] as the time zone and then press [ENTER] to return to the Enter Floor prompt.

```
Floor Grp 1 F1−01 F2−** F3−** F4−**
Enter Floor:
```

We suggest that each time you program or change a floor group, you record the details on the floor groups worksheet.

Option 21 Holidays

Overview

A holiday is a specified date (or range of dates) during which users are denied access during times that they would normally be permitted access. For example, a user may be able to disarm the system and unlock a door during working hours except on defined holidays.

Challenger can have 24 holiday records. Each record can be designated as recurring, so you don't need to reprogram a holiday if it falls on the same date each year.

Some users may require access during holidays. This functionality is provided via the time zone in the user's alarm group that allows access during holidays (via the holiday type).

Holidays have one or more holiday types numbered 1 to 8. For example, there might be four school holidays in a year, each of which has a Challenger holiday record to record the dates. If each of these holidays is designated as holiday type 1, then the holiday type provides access during school holidays, but not for other types of holidays (such as public holidays).

We suggest that you record the details of holidays and holiday types on the Holidays Worksheet (see "Holidays worksheet" on page 54).

Programming a holiday

From the User menu prompt (see "Using the keypad" on page 7), press [2] [1] [ENTER] to program a holiday.

```
Holidays
Holiday No:
```

Defining the start

Enter a holiday number in the range 1 to 24 and then press [ENTER]. The holiday programming screen displays.

```
Holiday 1:00/00/00−00/00/00
Start Day:
```

Enter a number in the range 1 to 31, and then press [ENTER] to program the day that the holiday begins.

```
Holiday 1:31/00/00−00/00/00
Start Mth:
```

Enter a number in the range 1 to 12, and then press [ENTER] to program the month in which the holiday begins.

```
Holiday 1:31/12/00−00/00/00
Start Yr:
```

Enter a number in the range 0 to 99, and then press [ENTER] to program the last two digits of the year in which the holiday begins.

Defining the end

A holiday can span a range of dates: if so, you need to program the end date. If the holiday is for only a single date, you can program only the start date, and then enter zeros for the day, month, and year of the end date.

```
Holiday 1:31/12/18−00/00/00
End Day:
```

Enter a number in the range 1 to 31, and then press [ENTER] to program the day that the holiday ends. Alternatively, enter 0 if this is a one-day holiday.

```
Holiday 1:31/12/18−02/00/00
End Mth:
```

Enter a number in the range 1 to 12, and then press [ENTER] to program the month in which the holiday ends. Alternatively, enter 0 if this is a one-day holiday.

```
Holiday 1:31/12/18−02/01/00
End Yr:
```

Enter a number in the range 0 to 99, and then press [ENTER] to program the last two digits of the year in which the holiday ends. Alternatively, enter 0 if this is a one-day holiday.

Assigning holiday types

A holiday must be assigned at least one holiday type in order for it to be used. The holiday type can be linked to a time zone. A holiday without a holiday type is inactive.

```
Holiday 1: Hol Types:
Type (1) − (8):
```

To assign a holiday type to a holiday, enter the holiday type number and then press [ENTER]. The holiday type number will display in the top line of the LCD screen.

Alternatively, to remove a holiday type from a holiday (it’s already displayed in the top line of the LCD screen), enter the number, and then press [ENTER].

Recurring holidays

```
NO − Recurring Holidays
*−Change 0−Skip
```

If required, press [MENU*] to toggle the programmed value from NO to YES, and then press [ENTER]. Alternatively, press [0] to exit this holiday.

When a future holiday is defined as recurring, then the year portion of the start and end dates is automatically incremented by 1 each time the holiday ends.

Option 22 Open Door

From the User menu prompt (see “Using the keypad” on page 7), press [2] [2] [ENTER] to unlock a door that you (and the RAS) are authorized to unlock.

The Open Door command would typically be used at a RAS that’s at a different location from the door (for example, from a security desk).

```
Open Door
Door No:
```

Enter the door number in the range 1 to 128 and then press [ENTER]. Alternatively, press [ENTER] to exit this option.

Option 23 Unlock, Lock, Disable and Enable

From the User menu prompt (see “Using the keypad” on page 7), press [2] [3] [ENTER] to unlock, timed unlock, lock, disable, or enable an intelligent door (doors numbered in the range 17 to 64 or 81 to 128 connected to an Intelligent Access Controller).

The door will remain in the state selected until an opposite event occurs in the system that will change the state of that door. For example, door 21 automatically unlocks at 8 a.m. and relocks at 5 p.m. by using an override time zone. If the user wishes to secure the premises and leave at 4 p.m., the door can be locked using the lock option, but will still automatically unlock at 8 a.m. again the following morning.

```
1−Unlock 2−Lock 3−Disable 4−Enable
Option:
```

Select an option:

- Press [1] [ENTER] to unlock a door.
- Press [2] [ENTER] to lock a door.
- Press [3] [ENTER] to disable a door.
- Press [4] [ENTER] to enable a door.
- Press [ENTER] to exit this option.

The following example uses option 1. The other options are similar.

Use 1–Unlock to unlock a door that you are authorized (via the door group assigned to your PIN code) to unlock.

```
Unlock Door
Door No:
```

Enter the door number (17 to 64 or 81 to 128) and then press [ENTER]. Alternatively, press [ENTER] to return to the User menu.

Option 24 Automation Control

From the User menu prompt (see “Using the keypad” on page 7), press [2] [4] [ENTER] to manually control an automation zone (such as lighting).

An automation zone is one or more building devices (including C-Bus® devices) that can be controlled via the Challenger system. 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 8 below depicts the RAS display for automation zone 1 named “Entrance lights”.

Figure 8: 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.

Automation Control via Quick Control

Quick control uses the CA111x RAS’s multi-function key (Figure 1 on page 4, item 3) as a shortcut to the automation zone control screen (Figure 8 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 order to prevent unauthorised use.

Option 25 Change PIN

From the User menu prompt (see “Using the keypad” on page 7), press [2] [5] [ENTER] to manually change users PIN.

This option enables users to change their own PIN code using the RAS to ensure the security of their account.

The Change PIN feature will perform some basic checks when a new PIN is entered, including verifying the existing PIN is correct for the user who is accessing this option and making sure the new PIN entered is correct and not already assigned to another user.

You may only change your own PIN code using this menu. In order to change other user’s PIN, please refer to Option 14 Program Users.

25- Change PIN

Enter the old code. It should match the code which has been entered when accessing the menus to get to this user option.

Enter old code
for 50 TECOM
Master
PIN: **

Enter the new code.

Enter new code
for 50 TECOM
Master
PIN: **

Re-Enter the new code.

This step has been put in place to ensure that you do not accidentally type in an incorrect PIN. Once you have entered the new PIN again, it will be active immediately.

Re-Enter new code
for 50 TECOM
Master
PIN: **

Code Changed
for 50 TECOM
Master Press

To confirm that the new PIN has been set correctly, exit the menus and then attempt to re-enter them using your new PIN.

Appendix A
Programming worksheets

Summary

Print or copy the following worksheets as needed.

Users worksheet

User records are programmed in user menu option 14. Program Users.

Figure 9: Users worksheet

Door groups worksheet

Door groups are programmed in user menu option 20. Door and Floor Groups. Challenger*Plus* panels support 255 door groups.

Figure 10: Door groups 1 to 128 worksheet

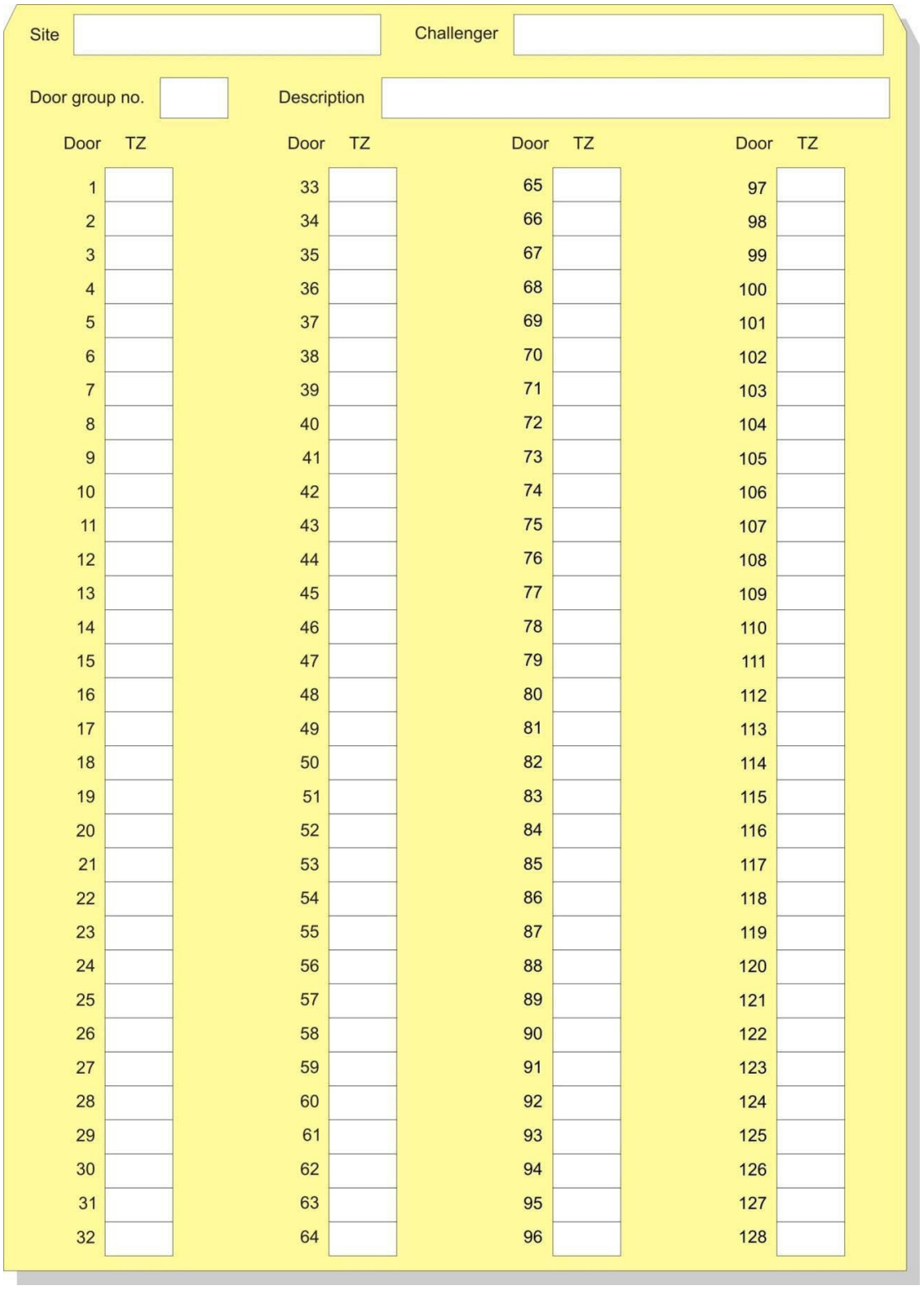
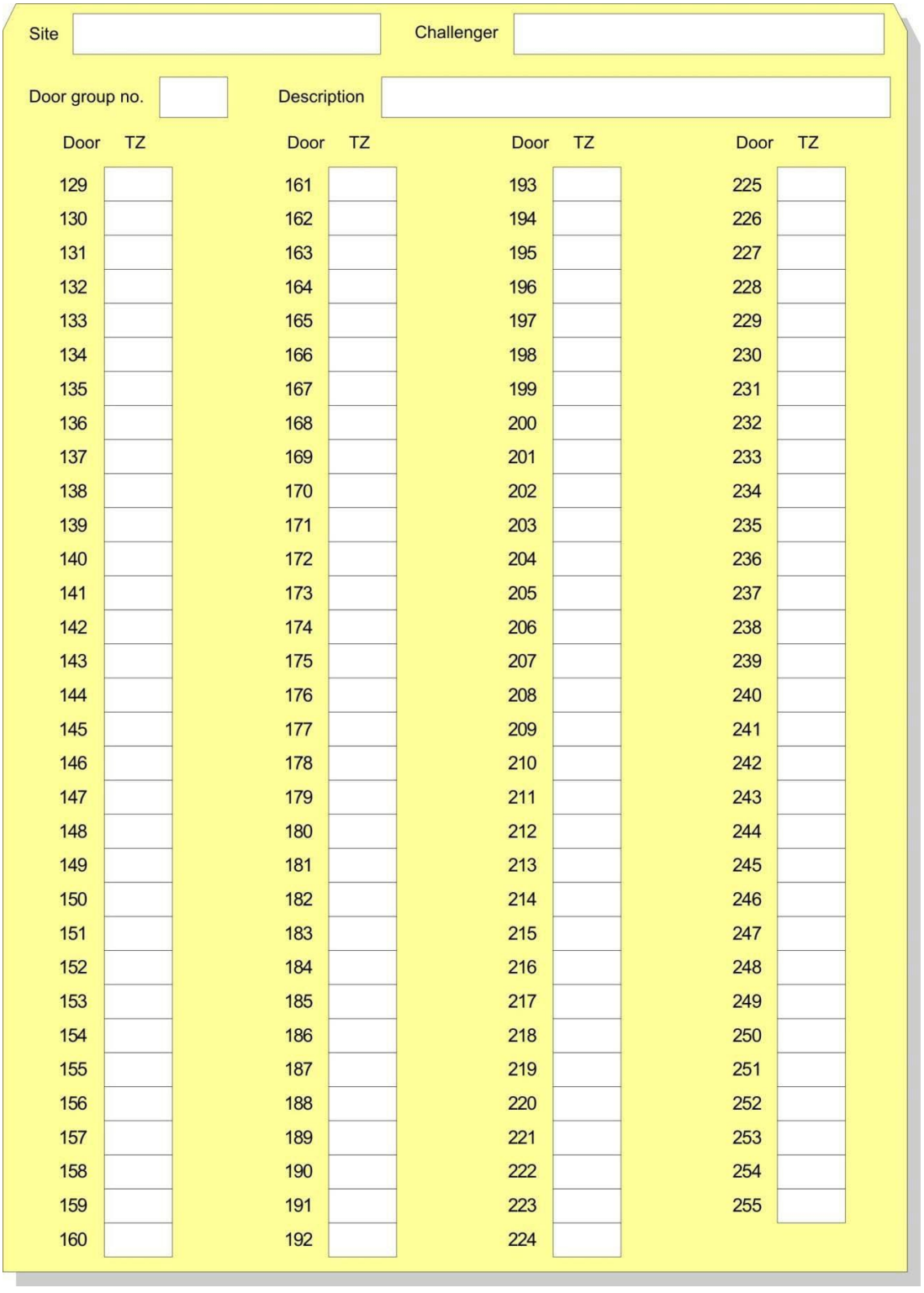


Figure 11: Door groups 129 to 255 worksheet



Site _____ Challenger _____

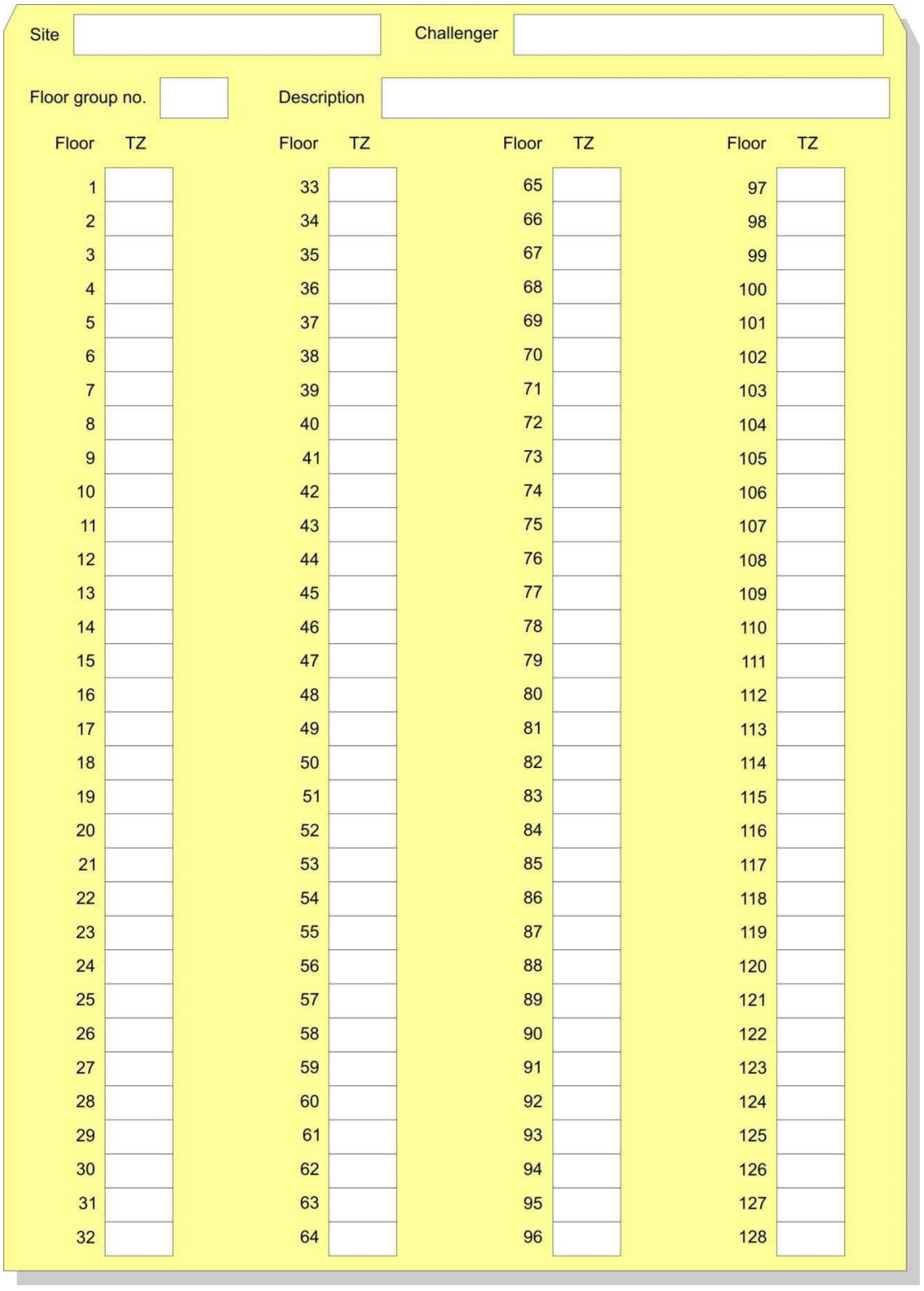
Door group no. _____ Description _____

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*Plus* panels support 128 floor groups.

Figure 12: Floor groups worksheet



Holidays worksheet

Holiday records are programmed in user menu option 21. Holidays.

Figure 13: Holidays worksheet

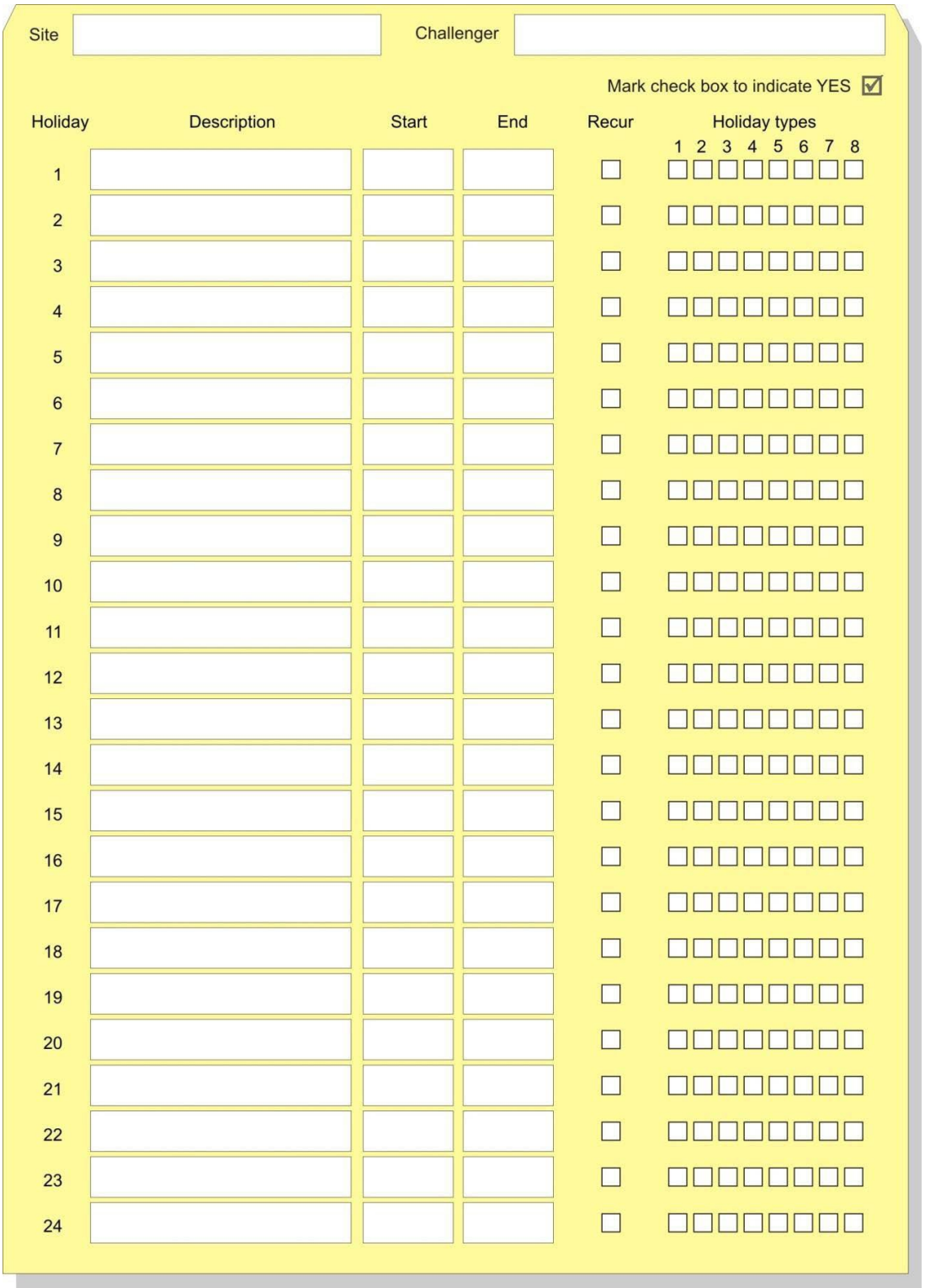


Figure 14: Holiday types worksheet

This page intentionally left blank

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 a 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, arming stations, 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 alarm events or other events to a remote monitoring company by means of a dialler and 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). **Note**: This functionality requires the use of 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.
Armed	See “*secure*”.
Arming station (RAS)	A device that provides a user interface for security functions for areas or for access points (doors). The arming station may be an LCD keypad, or any other device which can be used to perform security functions such as arm or disarm, open doors, and so on.
Automation control	A Challenger panel can control certain building devices such as lighting via automated programming or manual control via RAS.
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.
Central station	See “*remote monitoring company*”.
CID	Ademco Contact ID alarm reporting format.
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 requires the use of an Intelligent Access Controller.
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 requires the use of 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.
Extended access time	A longer than normal time for the door to unlock when a user with "Extended Access" presents a valid card or PIN at a door reader. **Note**: This functionality requires the use of 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 requires the use of an Intelligent Access Controller.
Guard	If the user is a “guard” type, then the system can generate a “guard failed to check in” alarm if required.
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 requires the use of 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 user code. **Note**: This functionality requires the use of 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.
Key switch	A device using a key-operated switch to arm or disarm areas.
Keypad	An arming station 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 system's two RS-485 data busses (LAN1 and LAN2).

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.
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 requires the use of 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 requires the use of 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 user code. **Note**: This functionality requires the use of 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 requires the use of an Intelligent Access Controller.
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 arming stations. Polling allows the remote unit to transfer data to the control panel.

RAS	Remote arming station. See “arming station”.
Reader	A device (arming station) 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 requires the use of 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).
Security Commander	Windows-based software that provides a large-scale, multi-operator, user interface to control small and large Challenger installations.
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”.
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*”.
Time zone	A time zone (or timezone) is a means of making certain Challenger functionality conditional. There are two types of time zones. 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.
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 timed arming and disarming functionality for specific areas.
User record	A record containing (at least) a user's PIN or card number to identify the user to the Challenger system.
Vault area	Vault areas are areas that, when armed, will automatically arm other areas after a specified time.
Visitor status	If the user flag “visitor status” is set to YES the user must be accompanied by a non-visitor user.
Zone input	See “*input*”.

This page intentionally left blank

Index